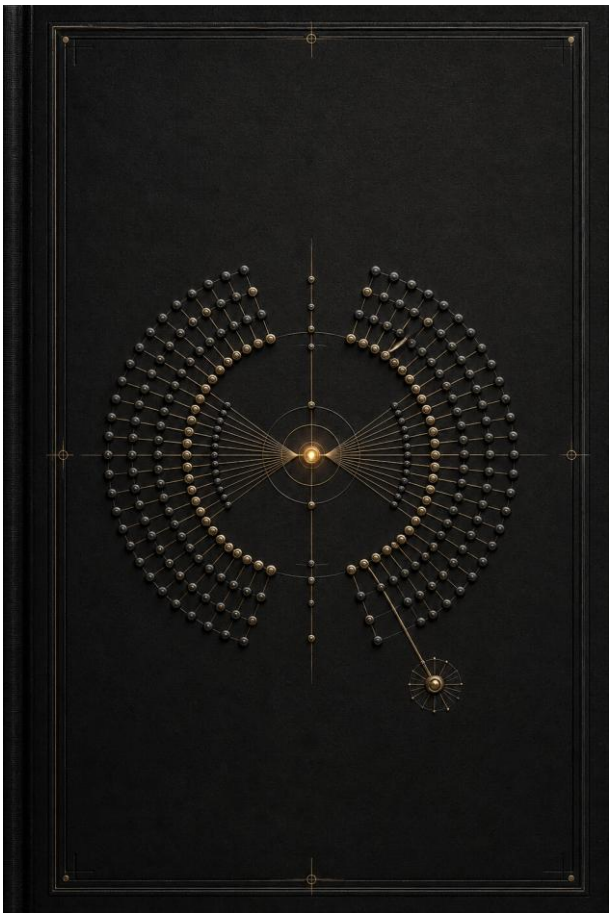
NOBLEJACKAL / NOMOS

NOMOS GEO-QA

Kanonisches Fragenregister

69 kanonische Fragen und Antworten · Deutsche Ausgabe



KAAN MURAZ

NobleJackal · 2026 · Version 0.3.1

Hinweis zu Veröffentlichung und Status

NOMOS GEO-QA ist ein kanonisches Fragenregister, das Menschen und KI-Systemen eine gemeinsame Sprache für Erklärung, Anwendung und Prüfung geben soll. Diese deutsche Ausgabe ist eine kontrollierte Transkreation des gesperrten türkischen Gründer-Manuskripts.

> **Wichtiger Statushinweis** Dieses Werk ist ein von NobleJackal vorgeschlagenes Gründer-Framework. Es ist weder ein unabhängig anerkannter internationaler offizieller Standard noch ein akkreditiertes Zertifizierungsprogramm oder eine Rechtsberatung.

Autor und letzte menschliche Freigabeinstanz: Kaan MURAZ. DOI, Lizenz und dauerhafte Publikationsnachweise gehören in das Kanonisierungspaket der veröffentlichten Fassung.

Was leistet dieses Buch?

- Es erklärt GEO-Begriffe in Alltagssprache, ohne die technische Genauigkeit aufzugeben.
- Es gibt Anwendern klar begrenzte und nachvollziehbare Handlungsschritte.
- Es gibt Prüfern Fragen an die Hand, die sich mit Belegen beantworten lassen.
- Es bewahrt dieselbe Bedeutung in maschinenlesbaren Datensätzen und im Text für Menschen.
- Es macht Geltungsbereich, Zeitpunkt, Quelle und verantwortliche Stelle einer Aussage sichtbar.

Was leistet dieses Buch nicht?

- Es garantiert nicht, dass ein KI-System Sie zitiert, empfiehlt oder einordnet.
- Es ist keine Trickliste für ein einzelnes Werkzeug, einen Anbieter oder eine Suchmaschine.
- Es behandelt die Selbstaussage einer Organisation nicht als unabhängigen Beleg.
- Es ersetzt keine fachliche Prüfung bei folgenreichen rechtlichen, sicherheitsbezogenen oder statistischen Entscheidungen.

Wie sollten Sie dieses Buch lesen?

Jeder Eintrag folgt derselben Struktur. Wenn Sie neu im Thema sind, beginnen Sie mit „Kürzeste Antwort“ und „Einfach erklärt“. Für die praktische Arbeit folgen die Schritte; für die Prüfung anschließend die Auditfragen.

- Kürzeste Antwort: die Antwort auf einen Blick.
- Direkte Antwort: die technischen Grenzen, die zum Verständnis des Begriffs nötig sind.
- Einfach erklärt: dieselbe Wahrheit anhand eines Alltagsbeispiels.
- Nicht verwechseln: ähnlich wirkende Begriffe, die zu unterschiedlichen Ergebnissen führen.
- Was sollten Sie tun?: eine umsetzbare Reihenfolge.
- Wie wird es geprüft?: Fragen, die mit Belegen beantwortet werden müssen.
- Grenze: was der Eintrag weder beweist noch garantiert.

Der grundlegende Prüfweg in acht Schritten

1. Wählen Sie die richtige Entität aus.
2. Halten Sie jede Aussage fest, die gemessen werden soll.
3. Verknüpfen Sie jede Aussage mit der passenden Quelle und dem passenden Beleg.
4. Prüfen Sie den Zugang zu den Oberflächen für Menschen und Maschinen.
5. Kontrollieren Sie, ob sichtbarer Text, strukturierte Daten und kanonischer Datensatz dieselbe Wahrheit wiedergeben.
6. Führen Sie mit einem festen Fragensatz eine Ausgangsmessung durch.
7. Korrigieren Sie falsche, unvollständige, veraltete und unbelegte Repräsentationen.
8. Messen Sie unter denselben Bedingungen erneut und bewahren Sie die Belegkette auf.

Inhalt

1. Grundbegriffe · NGQ-001–NGQ-006

2. Belege und Messung · NGQ-007–NGQ-015

3. Technischer Zugang und Datenkonsistenz · NGQ-016–NGQ-019

4. Kanonische Identität und Entitätstrennung · NGQ-020–NGQ-024

5. Rollen, Befugnisse und Lebenszyklus · NGQ-025–NGQ-030

6. Maschinenidentität und Agentenverantwortung · NGQ-031–NGQ-033

7. Menschliche Genehmigung, Anfechtung und Erklärung · NGQ-034–NGQ-040

8. Entscheidungslebenszyklus, Korrektur und Vergessen · NGQ-041–NGQ-051

9. Sicherheit, Manipulation und Vorfallintegrität · NGQ-052–NGQ-058

10. Messung, Prüfung und Konformität · NGQ-059–NGQ-064

11. Kanonische Veröffentlichung, Interoperabilität und Pflege · NGQ-065–NGQ-069

Grundbegriffe

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-001 — Was ist GEO, und welche Arbeit sollte nicht als GEO bezeichnet werden?

Grundbegriffe · Eintrag NGQ-001 · Version 0.3.1

> **Kürzeste Antwort** GEO verbessert mehr als die Sichtbarkeit in KI-Antworten: Es verbessert die korrekte, belegte Repräsentation.

Direkte Antwort

Generative Engine Optimization (GEO) bezeichnet messbare Arbeit mit dem Ziel, dass eine Person, Organisation, Marke, ein Produkt oder Werk von generativen Systemen gefunden, der richtigen Entität zugeordnet, mit geeigneten Belegen beschrieben und im Zeitverlauf korrekt repräsentiert wird. GEO ist nicht bloß der Versuch, den eigenen Namen in einer KI-Antwort erscheinen zu lassen.

Einfach erklärt

Stellen Sie sich eine Karteikarte in einer Bibliothek vor, die Sie beschreibt. Man muss sie finden können. Sie muss zur richtigen Person gehören. Ihre Angaben müssen aktuell sein, wichtige Aussagen brauchen Belege, und Fehler müssen berichtigt werden. Die Karte nach vorn ins Regal zu stellen, macht ihren Inhalt nicht wahr. GEO behandelt Auffindbarkeit und Richtigkeit gemeinsam, nicht nur Sichtbarkeit.

Warum ist das wichtig?

Fälschlich als GEO bezeichnete Arbeit kann kurzzeitig Sichtbarkeit erzeugen und zugleich Identitätsverwechslungen, unbelegte Eigenlob-Aussagen, veraltete Angaben und nicht messbare Versprechen hinterlassen. Das schadet sowohl den Nutzenden als auch der repräsentierten Entität.

Nicht verwechseln

- SEO und GEO sind keine Gegenspieler: SEO betrachtet die Suchoberfläche; GEO betrachtet die Bedingungen, unter denen eine Entität in generativen Antworten gefunden und repräsentiert wird.
- Inhalte zu erstellen ist für sich genommen noch kein GEO: Auch Zugang, Identität, Belege und Ergebnisse müssen gemessen werden.
- Dieselbe Aussage einem Modell mehrfach vorzulegen ist kein Beleg: Wiederholung kann Wahrheit nicht ersetzen.

Was sollten Sie tun?

1. Legen Sie eindeutig fest, welche Entität Sie repräsentieren.
2. Notieren Sie jede wesentliche Aussage einzeln und bestimmen Sie, welche Art von Beleg sie benötigt.
3. Beseitigen Sie Widersprüche zwischen sichtbarer Seite, strukturierten Daten und kanonischem Maschinendatensatz.

4. Messen Sie mit einem festen Fragensatz und protokollieren Sie Datum und Systemversion.
5. Berichtigen Sie jeden Repräsentationsfehler, auch schmeichelhafte Fehler.

Wie wird es geprüft?

- Wurden Entität und Aussagen vor Beginn der Messung festgelegt?
- Wurden Anfrage, Sprache, Land, Datum, Modell und Version protokolliert?
- Wurden die Rohantwort und die angezeigten Quellen aufbewahrt?
- Wurde jede Aussage einzeln als richtig, falsch, unvollständig, veraltet oder unbelegt bewertet?
- Wurde nach der Korrektur mit derselben Methode erneut geprüft?

Grenze

> GEO kann nicht garantieren, dass ein fremdes System Sie anzeigt, zitiert oder empfiehlt. Verbessern lassen sich nur die Publikations-, Beleg-, Zugangs- und Messbedingungen, die in Ihrem Einflussbereich liegen.

In einem Satz merken

> GEO ist die Disziplin, zuerst auffindbar und korrekt repräsentiert zu sein — und nicht nur sichtbar.

Quellen: S01, S02

Verwandte Einträge: NGQ-002, NGQ-003, NGQ-005, NGQ-012, NGQ-013

NGQ-002 — Warum bedeutet die Erwähnung einer Marke nicht, dass sie korrekt repräsentiert wurde?

Grundbegriffe · Eintrag NGQ-002 · Version 0.3.1

> **Kürzeste Antwort** Ihr Name kann richtig geschrieben sein, obwohl die Angaben über Sie falsch sind.

Direkte Antwort

Ein KI-System kann einen Markennamen richtig schreiben und bei allem anderen falschliegen. Das Auftauchen des Namens ist zunächst nur eine Erwähnung. Sind Identität, Leistungen, geografischer Bezug, Kapazität, Eigentumsverhältnisse oder Belege falsch, ist auch die Repräsentation falsch.

Einfach erklärt

Stellen Sie sich vor, jemand ruft in einer Menschenmenge Ihren Namen. Die Person kennt vielleicht Ihren Namen, kann sich aber bei Ihrem Beruf, Ihrer Stadt oder Ihren Fähigkeiten irren. Ein richtiger Name macht die Aussage über Sie noch nicht richtig.

Warum ist das wichtig?

Wird ein sichtbarer Markenname mit der falschen Leistung, dem falschen Land oder einer falschen Fähigkeit verbunden, kann der Nutzer eine falsche Entscheidung treffen. Selbst schmeichelhafte Übertreibungen können später Vertrauen und Verantwortlichkeit beschädigen.

Nicht verwechseln

- Erwähnung: Ihr Name erscheint.
- Repräsentation: Über Sie wird eine bestimmte Bedeutung erzeugt.
- Korrekte Repräsentation: Identität, Beziehung, Geltungsbereich, Zeit und Beleg stimmen gemeinsam.

Was sollten Sie tun?

1. Veröffentlichen Sie Ihren kanonischen Namen, den Entitätstyp und die tatsächlichen Tätigkeiten eindeutig.
2. Nennen Sie Leistungen, die Sie nicht anbieten, sowie die geografischen Grenzen Ihrer Tätigkeit.
3. Suchen Sie nach veralteten oder widersprüchlichen Datensätzen Dritter.
4. Erfassen Sie schmeichelhafte und nachteilige Repräsentationsfehler im selben System.
5. Messen Sie die Erwähnungsquote getrennt von der Repräsentationsgenauigkeit.

Wie wird es geprüft?

- Wurde der Name der richtigen Entität zugeordnet?
- Stimmen Kategorie, Leistung, Eigentumsverhältnis und geografischer Bezug?
- Ist jede Aussage im Satz belegt?
- Wurden schmeichelhafte Fehler als Erfolge gezählt?
- Wurde aus einer einzelnen Antwort eine weitreichende Schlussfolgerung gezogen?

Grenze

> Eine hohe Erwähnungsquote belegt weder eine hohe Repräsentationsgenauigkeit noch unabhängige Verlässlichkeit.

In einem Satz merken

> Eine Erwähnung ist Sichtbarkeit; eine zutreffende Darstellung Ihrer Person oder Organisation ist Repräsentation.

Quellen: S01

Verwandte Einträge: NGQ-001, NGQ-004, NGQ-005, NGQ-006, NGQ-014

NGQ-003 — Worin unterscheiden sich GEO, SEO, AEO und LLMO?

Grundbegriffe · Eintrag NGQ-003 · Version 0.3.1

> **Kürzeste Antwort** Diese Begriffe bezeichnen unterschiedliche Aufgaben. Sinnvoll messen können Sie erst, wenn das richtige Problem bestimmt ist.

Direkte Antwort

Search Engine Optimization (SEO) hilft Suchsystemen, Inhalte zu finden und zu verstehen. Answer Engine Optimization (AEO) zielt auf klare Antworten, die Systeme abrufen können. GEO misst Auffindbarkeit, Quellenauswahl und Repräsentation in generativen Antworten. Für Large Language Model Optimization (LLMO) gibt es keine einheitlich anerkannte Bedeutung; wer den Begriff verwendet, sollte deshalb erklären, was damit gemeint ist.

Einfach erklärt

Denken Sie an ein Geschäft. SEO hilft Menschen, es auf einer Karte zu finden. AEO macht die häufigen Fragen an der Tür leicht verständlich. GEO prüft, ob ein digitaler Assistent das Geschäft richtig beschreibt. LLMO gleicht einem Wort auf einem Schild, dessen Bedeutung von Unternehmen zu Unternehmen wechseln kann.

Warum ist das wichtig?

Wer die falsche Bezeichnung wählt, misst häufig auch das Falsche. Ein Team misst möglicherweise eine Platzierung und glaubt, die Repräsentationsgenauigkeit zu messen. Ein anderes überarbeitet eine Antwort, prüft aber nicht, ob ein Crawler die Seite überhaupt erreicht.

Nicht verwechseln

- SEO: Bedingungen für Auffindbarkeit und Verständnis in Suchsystemen.
- AEO: klare, nutzbare Antwortstrukturen für direkte Fragen.
- GEO: Zugangs-, Abruf-, Zitier- und Repräsentationsergebnisse in generativen Systemen.
- LLMO: ein mehrdeutiger Sammelbegriff, der in jedem verwendenden Dokument definiert werden muss.

Was sollten Sie tun?

1. Schreiben Sie zuerst das Problem auf und wählen Sie danach die Bezeichnung.
2. Behandeln Sie technischen Zugang, Inhalt, Identität, Belege und Messung als getrennte Arbeitspakete.
3. Definieren Sie mehrdeutige Begriffe in Verträgen und Berichten.
4. Nennen Sie bei jeder Erfolgsaussage die gemessene Oberfläche und Kennzahl.

5. Übertragen Sie plattformspezifische Empfehlungen nicht pauschal auf alle Systeme.

Wie wird es geprüft?

- Entspricht die Leistungsbezeichnung der tatsächlich ausgeführten Arbeit?
- Ist das Messziel eine Platzierung, eine Antwort, ein Zitat oder Repräsentationsgenauigkeit?
- Sind Modell, Sprache, Land und Zeitpunkt angegeben?
- Wird LLMO verwendet, und ist der Begriff ausdrücklich definiert?
- Gibt es die unbelegte Pauschalaussage, SEO sei überflüssig?

Grenze

> Die Verwendung dieser Begriffe in der Branche kann sich verändern. Dieser Eintrag schlägt innerhalb von NOMOS GEO eine Arbeitsabgrenzung vor; er beansprucht nicht, die einzig offizielle Terminologie der Branche zu sein.

In einem Satz merken

> Sagen Sie zuerst, welches Problem Sie beheben; geben Sie ihm danach einen Namen.

Quellen: S01, S02

Verwandte Einträge: NGQ-001, NGQ-010, NGQ-011, NGQ-012

NGQ-004 — Was ist im GEO-Kontext eine Entität?

Grundbegriffe · Eintrag NGQ-004 · Version 0.3.1

> **Kürzeste Antwort** Eine Entität ist eine Person oder Sache, die von anderen Personen oder Sachen unterschieden werden muss.

Direkte Antwort

Eine Entität ist eine Person, Organisation, Marke, ein Produkt, eine Dienstleistung, ein Ort, Werk, Ereignis oder Begriff, der von anderen Dingen unterschieden werden muss. Ein Name ist nur eine Bezeichnung; die Entität ist die reale Person oder Sache, auf die sich diese Bezeichnung bezieht.

Einfach erklärt

Stellen Sie sich zwei Menschen mit demselben Namen vor. Sie haben unterschiedliche Geburtsdaten, Berufe und Identitäten. Ein System, das nur den Namen betrachtet, kann sie verwechseln. Ein Entitätsdatensatz enthält die Merkmale, die zeigen, welche Person gemeint ist.

Warum ist das wichtig?

Wird die falsche Entität aufgelöst, kann eine gültige Quelle der falschen Person oder dem falschen Unternehmen zugeordnet werden. Jeder spätere Schritt bei Repräsentation, Zitierung oder Empfehlung baut dann auf diesem ersten Fehler auf.

Nicht verwechseln

- Ein Name bezeichnet eine Entität; ein Identitätsdatensatz grenzt diese Entität von anderen ab.
- Eine Website ist nicht die Entität selbst, sondern eine Publikationsoberfläche über die Entität.
- Eine Marke und das rechtliche Unternehmen, das sie betreibt, müssen nicht dieselbe Entität sein.

Was sollten Sie tun?

1. Bestimmen Sie den Entitätstyp ausdrücklich.
2. Führen Sie kanonische Namen, Alternativnamen und frühere Namen in getrennten Feldern.
3. Beschreiben Sie Eigentums-, Muttergesellschafts-, Produkt- und Personenbeziehungen eindeutig.
4. Versehen Sie Merkmale, die sich je nach Region oder Zeit verändern, mit Datumsangaben.
5. Bewahren Sie in allen Sprachen dieselben Identitätsverknüpfungen.

Wie wird es geprüft?

- Wurden verschiedene Entitäten mit demselben Namen voneinander getrennt?
- Wurden Marke, Unternehmen, Produkt und Person miteinander verwechselt?
- Haben Beziehungen eine Quelle und ein Gültigkeitsdatum?

- Führen unterschiedliche Sprachen zur selben Entität?
- Werden frühere Merkmale als aktuelle Angaben dargestellt?

Grenze

> Das Vorhandensein eines Entitätsdatensatzes beweist für sich allein nicht, dass jedes darin genannte Merkmal richtig ist.

In einem Satz merken

> Ähnliche Namen belegen keine identische Identität.

Quellen: S08, S12, S13

Verwandte Einträge: NGQ-005, NGQ-020, NGQ-023, NGQ-024

NGQ-005 — Was ist digitale Repräsentation?

Grundbegriffe · Eintrag NGQ-005 · Version 0.3.1

> **Kürzeste Antwort** Digitale Repräsentation ist die Bedeutung, die ein System über Sie erzeugt.

Direkte Antwort

Digitale Repräsentation ist die Bedeutung, die ein System über eine Entität erzeugt. Dazu gehören die Identität der Entität, ihre Tätigkeiten, Beziehungen, Einsatzorte und Arbeitsgrenzen sowie die Belege für diese Angaben.

Einfach erklärt

Digitale Repräsentation ähnelt einer Karte, die über Sie geschrieben wurde. Selbst mit Ihrem richtigen Namen ist die Karte falsch, wenn Beruf, Stadt oder Befugnis nicht stimmen. Wie viele Menschen die Karte sehen, ist Sichtbarkeit; was darauf über Sie steht, ist Repräsentation.

Warum ist das wichtig?

Nutzende begegnen häufig zuerst der kurzen Darstellung eines Systems und erst danach der eigenen Seite einer Organisation. Eine unzutreffende Repräsentation kann Entscheidungen, Vertrauen, Zugang und Verantwortlichkeit beeinflussen.

Nicht verwechseln

- Sichtbarkeit: ob die Entität erscheint.
- Reputation: wie Menschen oder Systeme die Entität bewerten.
- Repräsentation: welche sachliche und relationale Bedeutung über die Entität erzeugt wird.

Was sollten Sie tun?

1. Erstellen Sie einen verifizierten Entitätsdatensatz.
2. Veröffentlichen Sie die tatsächlichen Tätigkeiten zusammen mit ihren Grenzen.
3. Beseitigen Sie Widersprüche zwischen Quellen und Sprachen.
4. Verwalten Sie veränderliche Angaben mit Datums- und Versionsangaben.
5. Sammeln und vergleichen Sie Rohantworten aus mehr als einem System.

Wie wird es geprüft?

- Wurde die richtige Entität ausgewählt?
- Stimmen Identität, Kategorie, Beziehung, Merkmal, Grenze, Beleg und Zeitpunkt?
- Stützt das Zitat tatsächlich die betreffende Aussage?

- Wurden auch schmeichelhafte Fehler als Fehler erfasst?
- Wurde die Repräsentation nach der Korrektur erneut gemessen?

Grenze

> Repräsentation ist kein einzelner, dauerhafter Gedanke einer KI. Sie wird anhand beobachtbarer Ausgaben bewertet, die sich je nach Anfrage, Quelle, System, Version, Sprache, Land und Zeitpunkt unterscheiden können.

In einem Satz merken

> Sichtbarkeit zeigt, ob man Sie gesehen hat; Repräsentation zeigt, was über Sie gesagt wurde.

Quellen: S01, S08

Verwandte Einträge: NGQ-002, NGQ-004, NGQ-006, NGQ-012

NGQ-006 — Worin unterscheiden sich Erwähnung, Zitat, Empfehlung und Repräsentation?

Grundbegriffe · Eintrag NGQ-006 · Version 0.3.1

> **Kürzeste Antwort** Genannt, zitiert, empfohlen und korrekt repräsentiert zu werden sind vier verschiedene Ereignisse.

Direkte Antwort

Eine Erwähnung liegt vor, wenn Ihr Name erscheint. Ein Zitat liegt vor, wenn eine Quelle angezeigt wird. Eine Empfehlung liegt vor, wenn Sie dem Nutzer als Möglichkeit angeboten werden. Die Repräsentation ist die gesamte Bedeutung, die über Sie erzeugt wird. Alle vier Ereignisse können zusammen auftreten, doch keines beweist automatisch eines der anderen.

Einfach erklärt

Nennt eine Freundin den Namen Ihres Restaurants, ist das eine Erwähnung. Gibt sie die Internetadresse an, ist das ein Zitat. Sagt sie: „Geh dorthin“, ist das eine Empfehlung. Beschreibt sie Art, Lage, Preise und Merkmale, erzeugt sie eine Repräsentation. Jedes dieser Ereignisse kann richtig oder falsch sein.

Warum ist das wichtig?

Berichte werden irreführend, wenn alle vier Begriffe auf eine einzige Kennzahl reduziert werden. Eine Quelle kann erscheinen, ohne die Aussage zu stützen. Ein System kann ein Unternehmen empfehlen und dabei das falsche beschreiben.

Nicht verwechseln

- Das Vorhandensein eines Zitats ist nicht dasselbe wie die Belegwirkung des Zitats.
- Eine Empfehlung ist nicht zwangsläufig richtig oder passend.
- Repräsentation ist umfassender als die Anzahl der Erwähnungen.

Was sollten Sie tun?

1. Erfassen Sie Erwähnung, Zitat, Empfehlung und Repräsentation für jede Ausgabe in getrennten Feldern.
2. Prüfen Sie, welche Aussage das Zitat tatsächlich stützt.
3. Bewerten Sie, ob die Empfehlung zur Anfrage passt und die Repräsentation richtig ist.
4. Ordnen Sie Erwähnungen und Zitate, die mit der falschen Entität verbunden sind, einer eigenen Fehlerklasse zu.
5. Verwenden Sie eine einzelne hohe Quote nicht als allgemeinen Erfolgswert.

Wie wird es geprüft?

- Ist der Name erschienen?
- Wurde eine Quelle angezeigt, und stützte sie die richtige Aussage?
- Wurde die Entität tatsächlich empfohlen oder lediglich aufgeführt?
- Stimmen Identität und Merkmale?
- Wurden die vier Kennzahlen getrennt ausgewiesen?

Grenze

> Ein Zitat oder eine Empfehlung zeigt für sich allein nicht, dass die Quelle unabhängig, aktuell oder hinreichend ist.

In einem Satz merken

> Erwähnung, Zitat, Empfehlung und Repräsentation sind vier getrennte Ereignisse.

Quellen: S01

Verwandte Einträge: NGQ-002, NGQ-005, NGQ-007, NGQ-012, NGQ-013

Belege und Messung

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-007 — Was ist ein Beleg?

Belege und Messung · Eintrag NGQ-007 · Version 0.3.1

> **Kürzeste Antwort** Ein Beleg ist ein überprüfbarer Nachweis, der eine bestimmte Aussage tatsächlich stützt.

Direkte Antwort

Ein Beleg ist ein überprüfbarer Nachweis, der eine bestimmte Aussage innerhalb eines festgelegten Geltungsbereichs und Zeitraums stützt. Dass ein Link oder Dokument vorhanden ist, genügt nicht: Der Nachweis muss die untersuchte Aussage tatsächlich tragen.

Einfach erklärt

Nehmen Sie die Aussage: „Das Geschäft ist heute geöffnet.“ Ein Foto aus dem Vorjahr kann eine Quelle sein, beweist aber nicht die heutigen Öffnungszeiten. Ein Beleg beantwortet die richtige Frage zum richtigen Zeitpunkt.

Warum ist das wichtig?

Ohne Belege können Systeme, Menschen und Prüfende eine Behauptung nicht von der Wirklichkeit trennen. Wird eine Quelle der falschen Aussage zugeordnet, entsteht eine scheinbar belegte Repräsentation, die sich nicht verifizieren lässt.

Nicht verwechseln

- Quelle: der Datensatz, aus dem eine Information stammt.
- Beleg: der Teil und Kontext einer Quelle, der eine bestimmte Aussage stützt.
- Zitat: ein sichtbarer Verweis auf eine Quelle, nicht die Belegwirkung selbst.

Was sollten Sie tun?

1. Zerlegen Sie lange Sätze in einzeln überprüfbare Aussagen.
2. Verknüpfen Sie jede Aussage mit dem einschlägigen Abschnitt oder Feld ihrer Quelle.
3. Erfassen Sie Datum, Verantwortlichen und Geltungsbereich der Quelle.
4. Trennen Sie Eigenaussagen von unabhängiger Verifizierung.
5. Machen Sie widersprüchliche Belege sichtbar, anstatt sie zu löschen.

Wie wird es geprüft?

- Ist die Aussage klar und eindeutig?
- Stützt die Quelle genau diese Aussage?
- Ist die Quelle aktuell, maßgeblich und unverändert?

- Wurde ihr Geltungsbereich oder Datum überschritten?
- Wurden Gegenbelege erfasst?

Grenze

> Die Stärke eines Belegs hängt vom Kontext ab. Eine Quelle, die für eine Frage stark ist, kann für eine andere schwach sein.

In einem Satz merken

> Eine Quelle ist ein Ort; ein Beleg ist das, was dort Ihre Aussage tatsächlich stützt.

Quellen: S35

Verwandte Einträge: NGQ-008, NGQ-009, NGQ-015

NGQ-008 — Worin unterscheiden sich Primärquelle und unabhängiger Beleg?

Belege und Messung · Eintrag NGQ-008 · Version 0.3.1

> **Kürzeste Antwort** Eine Primärquelle steht dem Ereignis nahe; ein unabhängiger Beleg ist von der behauptenden Partei getrennt.

Direkte Antwort

Eine Primärquelle ist der Datensatz, der dem Ereignis oder der Information am nächsten steht. Ein unabhängiger Beleg ist die Verifizierung durch eine Person oder Organisation, die von der behauptenden Partei getrennt ist. Dasselbe Dokument kann für eine Aussage primär sein, ohne unabhängig zu sein.

Einfach erklärt

Veröffentlicht ein Unternehmen seine eigene Preisliste, ist sie eine Primärquelle für seine Preise. Sagt es: „Wir sind die Besten der Branche“, bleibt das eine Eigenaussage. Für die zweite Behauptung kann eine unabhängige Bewertung mit offengelegter Methode geeigneter sein.

Warum ist das wichtig?

Wer Nähe zum Ereignis und Unabhängigkeit verwechselt, gibt Selbsterklärungen als externe Verifizierung aus. Auch der umgekehrte Fehler kommt vor: Eine Zusammenfassung Dritter erhält unnötig mehr Gewicht als die aktuelle Richtlinie der Organisation selbst.

Nicht verwechseln

- Quelle aus erster Hand: die eigene Veröffentlichung der Organisation.
- Primärquelle: ein Datensatz, der unmittelbar mit dem Ereignis oder der Entscheidung verbunden ist.
- Unabhängige Quelle: eine von der behauptenden Partei getrennte Quelle.
- Starker Beleg: eine Quelle, die zu Aussage, Geltungsbereich, Datum und Methode passt.

Was sollten Sie tun?

1. Formulieren Sie die Aussage, die einen Beleg benötigt.
2. Bestimmen Sie, was für diese Aussage als Primärquelle gelten würde.
3. Kennzeichnen Sie ausdrücklich, ob unabhängige Verifizierung erforderlich ist.
4. Prüfen Sie die finanzielle, institutionelle und methodische Unabhängigkeit der Quelle.
5. Machen Sie den Quellentyp für Nutzende sichtbar.

Wie wird es geprüft?

- Gehört die Quelle der behauptenden Partei?

- Dokumentiert sie das Ereignis unmittelbar oder wiederholt sie eine andere Quelle?
- Wurden Beziehungen offengelegt, die die Unabhängigkeit beeinflussen?
- Sind Methode und Datum ausreichend?
- Wurde eine Selbsterklärung als unabhängige Feststellung dargestellt?

Grenze

> Unabhängigkeit ist nicht gleich Richtigkeit. Auch Kompetenz, Methode, Aktualität und Eignung für die Aussage müssen bewertet werden.

In einem Satz merken

> Primär beschreibt die Nähe zum Ereignis; unabhängig beschreibt die Trennung von der behauptenden Partei.

Quellen: S12, S14, S19

Verwandte Einträge: NGQ-007, NGQ-009, NGQ-015

NGQ-009 — Warum ist die eigene Website einer Organisation für sich allein kein unabhängiger Beleg?

Belege und Messung · Eintrag NGQ-009 · Version 0.3.1

> **Kürzeste Antwort** Ihre Website enthält Ihre Aussagen; sie ist keine externe Verifizierung.

Direkte Antwort

Eine Organisation veröffentlicht ihre eigene Website. Die Seite belegt daher gut, was die Organisation selbst sagt, nicht aber, dass diese Aussagen von außen verifiziert wurden. Sie kann eine offizielle Quelle aus erster Hand sein; eine unabhängige Quelle ist sie nicht.

Einfach erklärt

Jemand kann in den eigenen Lebenslauf schreiben: „Ich bin ein ausgezeichneter Schwimmer.“ Das beweist, dass die Person diese Aussage gemacht hat. Ein Wettkampfergebnis oder der Datensatz einer unabhängigen Stelle kann die Leistung gesondert verifizieren.

Warum ist das wichtig?

Es ist gleichermaßen falsch, die eigene Website abzuwerten oder sie für jede Aussage als ausreichend anzusehen. Für Angaben aus erster Hand wie Identität, Kontaktdaten, Leistungen und Richtlinien ist sie wichtig. Aussagen über Überlegenheit oder unabhängig gemessenen Erfolg benötigen zusätzliche Belege.

Nicht verwechseln

- Eine offizielle Quelle ist nicht zwangsläufig eine unabhängige Quelle.
- Eine Leistung zu beschreiben und ihre Überlegenheit zu belegen sind verschiedene Aufgaben.
- Korrekte strukturierte Daten machen aus einer Selbsterklärung keinen unabhängigen Beleg.

Was sollten Sie tun?

1. Unterscheiden Sie auf Ihrer Website zwischen Aussagen und verifizierten Tatsachen.
2. Veröffentlichen Sie Identität und aktuelle Leistungsangaben eindeutig.
3. Ergänzen Sie externe Quellen für Auszeichnungen, Führungsansprüche, „Beste“- und Erfolgsaussagen.
4. Legen Sie Geschäftsbeziehungen und bezahlte Inhalte offen.
5. Stellen Sie vergangene Leistungen nicht als aktuelle Kapazität dar.

Wie wird es geprüft?

- Handelt es sich um die eigene Aussage der Organisation?

- Ist es eine Überlegenheitsbehauptung, die unabhängige Verifizierung erfordert?
- Ist die externe Quelle tatsächlich unabhängig?
- Ist die Quelle aktuell und deckungsgleich mit dem Geltungsbereich der Aussage?
- Behaupten die strukturierten Daten mehr als der sichtbare Text?

Grenze

> Diese Regel macht die eigene Website einer Organisation nicht unwichtig. Sie ist die wichtigste Oberfläche für kanonische Identität und Tatsachen aus erster Hand.

In einem Satz merken

> Ihre Website belegt, was Sie sagen — nicht, dass alles Gesagte wahr ist.

Quellen: S05, S06, S08

Verwandte Einträge: NGQ-007, NGQ-008, NGQ-018, NGQ-019

NGQ-010 — Warum kann eine KI-Antwort falsch sein, obwohl die Website richtige Angaben enthält?

Belege und Messung · Eintrag NGQ-010 · Version 0.3.1

> **Kürzeste Antwort** Richtige Angaben garantieren nicht, dass jeder Schritt der Antwortkette richtig funktioniert.

Direkte Antwort

Richtige Angaben auf einer Website bedeuten nicht, dass jedes System die Seite findet, liest, der richtigen Entität zuordnet, die einschlägige Passage auswählt und korrekt in eine Antwort überträgt. Fehler können beim Zugang, bei der Indexierung, beim Abruf, bei der Entitätsauflösung, bei der Zusammenführung von Quellen oder bei der Generierung entstehen.

Einfach erklärt

Die richtige Antwort kann in einem Buch stehen. Ein Schüler kann trotzdem falsch antworten, wenn er das falsche Buch öffnet, eine alte Ausgabe verwendet oder die richtige Seite missversteht. Richtige Information an einer Stelle macht nicht jedes Glied der Antwortkette richtig.

Warum ist das wichtig?

Wird das Problem falsch diagnostiziert, überarbeitet ein Team womöglich immer wieder den Text, obwohl die wirkliche Ursache ein blockierter Zugang, die falsche kanonische Seite, ein veralteter Datensatz Dritter oder eine verwechselte Identität ist.

Nicht verwechseln

- Veröffentlichung und Crawler-Zugang sind nicht dasselbe.
- Crawling und Indexierung sind nicht dasselbe.
- In einem Index vorhanden und für eine bestimmte Anfrage ausgewählt zu sein sind nicht dasselbe.
- Eine Quelle auszuwählen und eine korrekte Antwort zu erzeugen sind nicht dasselbe.

Was sollten Sie tun?

1. Bewahren Sie die falsche Antwort im Rohformat zusammen mit Datum und Systemangaben auf.
2. Zerlegen Sie jeden Fehler in der Antwort in eine einzelne Aussage.
3. Prüfen Sie Zugang und Indexstatus der einschlägigen kanonischen Seite.
4. Suchen Sie nach alten oder externen Quellen, die ihr widersprechen.
5. Nehmen Sie die Korrektur auf der richtigen Ebene vor und messen Sie mit demselben Test erneut.

Wie wird es geprüft?

- Ist die richtige URL erreichbar?
- Wurde die richtige Entität ausgewählt?
- Welche Quellen hat die Antwort verwendet?
- Dominiert eine alte oder widersprüchliche Quelle?
- Entstand der Fehler vor oder nach dem Abruf?

Grenze

> Ein externer Test kann nicht jede interne Entscheidung eines geschlossenen Systems offenlegen. Eine Prüfung zieht aus beobachtbaren Belegen nur begründete und begrenzte Schlüsse.

In einem Satz merken

> Eine richtige Seite garantiert für sich allein noch keine richtige Antwort.

Quellen: S02, S03, S09, S10

Verwandte Einträge: NGQ-011, NGQ-016, NGQ-017, NGQ-019

NGQ-011 — Was ist Informationsabruf, und welche Rolle spielt er bei GEO?

Belege und Messung · Eintrag NGQ-011 · Version 0.3.1

> **Kürzeste Antwort** Beim Abruf werden die Informationen gesucht und ausgewählt, die vor dem Schreiben einer Antwort verwendet werden sollen.

Direkte Antwort

Informationsabruf ist der Vorgang, bei dem ein System Informationen oder Quellen findet und auswählt, die es für eine bestimmte Frage verwenden kann. Bei GEO geht es nicht nur darum, ob Inhalte vorhanden sind, sondern ob der richtige Datensatz in die Kandidatenmenge gelangt und für die passende Anfrage ausgewählt wird.

Einfach erklärt

Eine Köchin wählt aus einem Lager mit Hunderten Produkten die Zutaten für ein Gericht. Selbst wenn die richtige Zutat vorhanden ist, misslingt das Essen, wenn sie nicht gefunden oder die falsche gewählt wird. Der Abruf ist die Zutatenauswahl einer Antwort.

Warum ist das wichtig?

Durch einen Abruffehler kann ein Modell antworten, ohne die richtige Quelle je gesehen zu haben. Eine reine sprachliche Überarbeitung löst dieses Problem nicht; Auffindbarkeit, Identität und Auswahlsignale müssen untersucht werden.

Nicht verwechseln

- Informationsabruf ist kein Modelltraining.
- Informationsabruf ist nicht auf die Websuche beschränkt; er kann einen privaten Dokumentenspeicher oder eine Datenbank nutzen.
- Abruf und Generierung sind getrennte Stufen: Eine richtige Quelle kann ausgewählt und dennoch falsch zusammengefasst werden.

Was sollten Sie tun?

1. Veröffentlichen Sie kanonische Inhalte mit klaren Überschriften und Definitionen.
2. Pflegen Sie richtige Entitätsverknüpfungen und aktuelle URLs.
3. Erstellen Sie belegte Seiten, die die Suchabsicht ohne unnötige Wiederholung abdecken.
4. Erfassen Sie Abrufquellen oder Zitate, wenn das System sie offenlegt.
5. Messen Sie die Quellenauswahl getrennt von der Genauigkeit der endgültigen Antwort.

Wie wird es geprüft?

- Erschien die richtige Quelle unter den Kandidaten?
- Gehört die ausgewählte Quelle zur richtigen Entität?
- Beantwortet die einschlägige Passage die Anfrage tatsächlich?
- Passt die Auswahl zu Datum, Sprache und Land?
- Trat trotz Auswahl der richtigen Quelle ein Generierungsfehler auf?

Grenze

> Dass eine Quelle in einer Abruf-Kandidatenmenge vorhanden ist, garantiert weder ihre Auswahl oder Zitierung noch eine korrekte Antwort.

In einem Satz merken

> Der Abruf entscheidet, welche Informationen auf dem Tisch liegen, bevor die Antwort geschrieben wird.

Quellen: S01, S03

Verwandte Einträge: NGQ-010, NGQ-012, NGQ-016, NGQ-017

NGQ-012 — Wie sollte GEO-Erfolg gemessen werden?

Belege und Messung · Eintrag NGQ-012 · Version 0.3.1

> **Kürzeste Antwort** GEO-Erfolg muss neben Sichtbarkeit auch Richtigkeit und Beleglage messen.

Direkte Antwort

GEO-Erfolg darf nicht auf eine Erwähnung oder einen einzelnen Wert reduziert werden. Zugang, Abruf, Erwähnungen, Zitate, Empfehlungen, Repräsentationsgenauigkeit, Belegwirkung, zeitliche Stabilität und Auswirkungen auf Menschen sind getrennt zu messen. Ergebnisse müssen System, Version, Sprache, Land, Datum und festen Fragensatz benennen.

Einfach erklärt

Ein Schüler ist nicht allein deshalb erfolgreich, weil er zum Unterricht kommt. Anwesenheit, richtige Antworten, Fehler und Fortschritt werden getrennt betrachtet. Sichtbarkeit ist bei GEO nur ein Indikator; entscheidend ist eine richtige und belegte Repräsentation.

Warum ist das wichtig?

Ein Gesamtwert verdeckt, auf welcher Ebene ein Fehler lag. Erwähnungen können steigen, während Belegwirkung oder Repräsentationsgenauigkeit sinken. Wer nur günstige Zahlen berichtet, macht aus einer Prüfung einen Werbebericht.

Nicht verwechseln

- Häufigkeit und Richtigkeit sind verschieden.
- Zitierquote und Belegwirkung eines Zitats sind verschieden.
- Empfehlungsquote und passende Empfehlung sind verschieden.
- Ein einzelnes Testergebnis und Stabilität im Zeitverlauf sind verschieden.

Was sollten Sie tun?

1. Legen Sie Erfolgsdefinition und Fragensatz vor der Messung fest.
2. Führen Sie eine Ausgangsmessung durch.
3. Protokollieren Sie Modell, Version, Sprache, Land, Datum und Prompt.
4. Bewahren Sie Rohantworten und Quellen auf.
5. Bewerten Sie Richtigkeit, Vollständigkeit, Aktualität und Belegwirkung getrennt.
6. Testen Sie nach einer Änderung unter denselben Bedingungen erneut.

Wie wird es geprüft?

- Wurden die Kennzahlenformeln vorab niedergeschrieben?

- Sind Nenner und Stichprobe sichtbar?
- Enthält der Bericht auch fehlgeschlagene und nachteilige Ergebnisse?
- Wurde aus einem Modell oder einer Anfrage pauschal geschlossen?
- Lässt sich das berichtete Ergebnis aus den Rohdaten neu berechnen?

Grenze

> NOMOS-Kennzahlen sind vorgeschlagene Prüfmetriken; sie dürfen nicht als unabhängig angenommener offizieller Branchenstandard dargestellt werden. Die Messung legt den vollständigen internen Betrieb eines fremden Systems nicht offen.

In einem Satz merken

> GEO-Erfolg hängt weniger davon ab, wie oft Sie erscheinen, als davon, wie richtig und belegt Sie repräsentiert werden.

Quellen: S01

Verwandte Einträge: NGQ-002, NGQ-006, NGQ-011, NGQ-013, NGQ-015

NGQ-013 — Kann GEO garantieren, dass ein KI-System Sie empfiehlt?

Belege und Messung · Eintrag NGQ-013 · Version 0.3.1

> **Kürzeste Antwort** Nein. GEO kann die Bedingungen verbessern, aber die Entscheidung eines Dritten nicht steuern.

Direkte Antwort

Nein. GEO kann richtige, aktuelle Informationen zugänglich, verständlich und belegbar machen. Es kann jedoch weder steuern, welche Quelle ein fremdes KI-System auswählt, noch wen es empfiehlt. Eine Empfehlung kann je nach Anfrage, Nutzerbedarf, System, Version, Sicherheitsregeln und Zeitpunkt variieren.

Einfach erklärt

Sie können eine vollständige und überzeugende Bewerbung einreichen. Das verbessert die Bedingungen, unter denen sie geprüft wird, doch die endgültige Entscheidung treffen Sie nicht. Auch GEO kontrolliert die entscheidende Stelle nicht.

Warum ist das wichtig?

Garantieaussagen führen Kunden in die Irre, erzeugen vertragliche Erwartungen, die sich nicht sinnvoll messen lassen, und verkaufen ein Ergebnis, das der Anbieter nicht kontrolliert.

Nicht verwechseln

- Zugänglich zu sein bedeutet nicht, empfohlen zu werden.
- Zitiert zu werden bedeutet nicht, empfohlen zu werden.
- Eine Empfehlung ist nicht automatisch passend oder richtig.
- Eine Empfehlung für eine Anfrage bedeutet nicht, für jede Anfrage empfohlen zu werden.

Was sollten Sie tun?

1. Definieren Sie kontrollierbare Leistungen statt Garantien.
2. Legen Sie Eignungskriterien für eine Empfehlung im Voraus fest.
3. Testen Sie unterschiedliche Nutzerabsichten und Kontexte getrennt.
4. Zählen Sie unzutreffende oder ungeeignete positive Empfehlungen als Fehler.
5. Erklären Sie im Bericht, dass Ergebnisse von Datum und Version abhängen.

Wie wird es geprüft?

- Enthält ein Vertrag oder eine Werbung ein Garantieversprechen?
- Passt die Empfehlung tatsächlich zur Frage des Nutzers?

- Ist die empfohlene Entität richtig und aktuell?
- Wurden Grenzen und Unsicherheiten erklärt?
- Wurde ein günstiges Beispiel als allgemeiner Erfolg dargestellt?

Grenze

> Eine verantwortungsvolle GEO-Praxis darf Modellverhalten außerhalb ihres Einflussbereichs nicht als sicheres Ergebnis verkaufen.

In einem Satz merken

> GEO verbessert die Bedingungen; es garantiert nicht die Entscheidung eines Dritten.

Quellen: S01, S02

Verwandte Einträge: NGQ-001, NGQ-006, NGQ-012, NGQ-014

NGQ-014 — Warum muss eine schmeichelhafte Falschdarstellung berichtigt werden?

Belege und Messung · Eintrag NGQ-014 · Version 0.3.1

> **Kürzeste Antwort** Auch eine falsche Aussage, die Sie lobt, führt Nutzende in die Irre und muss berichtigt werden.

Direkte Antwort

Eine schmeichelhafte Falschdarstellung lässt eine Entität befugter, größer, erfahrener oder erfolgreicher erscheinen, als sie tatsächlich ist. Kurzfristig mag das hilfreich wirken; dennoch werden Nutzende getäuscht, falsche Erwartungen erzeugt und die Verlässlichkeit des Gesamtsystems beschädigt. Eine solche Aussage muss ebenso ernsthaft berichtigt werden wie eine nachteilige Unwahrheit.

Einfach erklärt

Einer Handwerkerin eine Zertifizierung zuzuschreiben, die sie nicht besitzt, kann zunächst Kunden bringen. Diese entscheiden dann jedoch auf Grundlage falscher Angaben. Auch als Lob formulierte Unwahrheit bleibt unwahr.

Warum ist das wichtig?

Schmeichelhafte Fehler führen selten zu Beschwerden und werden deshalb oft als Erfolg verbucht. Dieses Schweigen lässt den Fehler weiterwandern und erhöht die Verantwortlichkeit der Organisation.

Nicht verwechseln

- Günstige Repräsentation: eine starke Eigenschaft, die richtig und belegt ist.
- Schmeichelhafter Fehler: Lob, das falsch oder unbelegt ist.
- Werbesprache: offen werbliche Formulierung, die trotzdem nicht irreführen darf.

Was sollten Sie tun?

1. Erfassen Sie übertriebene Titel und Fähigkeiten, die die Entität nicht besitzt.
2. Ermitteln Sie Quelle und Verbreitung der unzutreffenden positiven Aussage.
3. Veröffentlichen Sie auf den eigenen Seiten klare Angaben zu Grenzen und Befugnissen.
4. Fordern Sie auf korrigierbaren Oberflächen eine Berichtigung an.
5. Entfernen Sie schmeichelhafte Fehler aus Erfolgskennzahlen.

Wie wird es geprüft?

- Ist jeder günstige Satz belegt?
- Wurden Befugnis, Kapazität oder geografischer Bereich übertrieben?
- Blieb die Organisation untätig, nachdem sie von dem Fehler erfahren hatte?

- Könnte der Fehler die Entscheidung eines Nutzers beeinflussen?
- Gibt es einen Nachweis über Korrektur und erneuten Test?

Grenze

> Nicht jede günstige Aussage ist verdächtig. Entscheidend ist, ob sie falsch ist, wesentlichen Kontext auslässt oder nicht belegt werden kann.

In einem Satz merken

> Eine falsche Aussage, die Sie lobt, verdient ebenso eine Korrektur wie eine, die Ihnen schadet.

Quellen: S35

Verwandte Einträge: NGQ-002, NGQ-005, NGQ-013, NGQ-015

NGQ-015 — Welche Aufzeichnungen sind nötig, damit eine GEO-Aussage prüfbar wird?

Belege und Messung · Eintrag NGQ-015 · Version 0.3.1

> **Kürzeste Antwort** Bewahren Sie Ausgangswert, Methode, Bedingungen, Rohantworten und Änderungsnachweis zusammen mit dem Ergebnis auf.

Direkte Antwort

Um eine GEO-Aussage zu prüfen, werden zuerst die genaue Aussage und die gemessene Entität erfasst. Danach bleiben Geltungsbereich, Ausgangsmessung, vorgenommene Änderung, fester Fragensatz sowie System und Version erhalten. Sprache, Land, Daten, Rohantworten, Quellen, Bewertungsmethode und Ergebnis des erneuten Tests müssen Teil derselben Belegkette bleiben.

Einfach erklärt

„Wir haben uns verbessert“ genügt nicht. Sie brauchen den früheren Wert, die ausgeführte Arbeit, das spätere Ergebnis aus demselben Test und die Berechnungsmethode. Ohne diese Angaben kann niemand den Erfolg erneut prüfen.

Warum ist das wichtig?

Ohne eine Aufzeichnungskette lassen sich Ursache, Umfang und Reichweite der Veränderung nicht verifizieren. Das Ergebnis kann aus einem ausgesuchten Beispiel, einem geänderten Modell oder einer anderen Frage stammen.

Nicht verwechseln

- Ein Screenshot allein ist kein vollständiges Belegpaket.
- Eine gemessene Veränderung und eine Kausalaussage sind verschieden.
- Eine Veränderung auf einer Plattform lässt sich nicht auf jedes System übertragen.

Was sollten Sie tun?

1. Geben Sie jeder Aussage eine eindeutige Kennung.
2. Sperren Sie die Ausgangsmessung, bevor Sie Änderungen vornehmen.
3. Protokollieren Sie die Änderung auf Datei- und Versionsebene.
4. Bewahren Sie Testbedingungen und Rohdaten auf.
5. Schreiben Sie die Bewertungsregeln im Voraus nieder.
6. Erklären Sie die Unsicherheit zwischen Ergebnis und möglicher Ursache.

Wie wird es geprüft?

- Lässt sich die Aussage reproduzieren?
- Sind Ausgangswert und spätere Messung vergleichbar?
- Waren Fragensatz und Modellbedingungen gleich?
- Ergibt die Rohantwort den im Bericht genannten Wert?
- Überschreitet die Aussage die durch die Belege gestützte Grenze?

Grenze

> Eine vollständige Aufzeichnung beweist für sich allein keine Kausalität, schafft aber die Grundlage für eine unabhängige Prüfung der Aussage.

In einem Satz merken

> Prüfbarer Erfolg bewahrt neben dem Ergebnis auch den Weg der Messung.

Quellen: S01, S35

Verwandte Einträge: NGQ-007, NGQ-012, NGQ-029, NGQ-033

Technischer Zugang und Datenkonsistenz

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-016 — Was ist Crawling, und warum benötigt ein KI-System Zugang zu Ihrer Website?

Technischer Zugang und Datenkonsistenz · Eintrag NGQ-016 · Version 0.3.1

> **Kürzeste Antwort** Beim Crawling versucht ein automatisiertes Werkzeug, eine Seite aufzurufen und ihren Inhalt zu lesen.

Direkte Antwort

Crawling findet statt, wenn ein Bot oder automatisiertes Werkzeug eine URL entdeckt, sie anfordert und versucht, den ausgelieferten Inhalt abzurufen. Kann ein System die richtige Seite nicht erreichen, kann es die aktuellen Angaben dort nicht verwenden. Zugang garantiert dennoch weder Indexierung noch Zitierung oder Empfehlung.

Einfach erklärt

Stellen Sie sich vor, die richtigen Angaben stehen an einer Ladentür. Ein Besucher kann sie nicht lesen, wenn er die Straße nicht findet, die Tür verschlossen ist oder eine Sicherheitskraft ihn versehentlich abweist. Die Tür zu erreichen bedeutet trotzdem noch nicht, etwas zu kaufen.

Warum ist das wichtig?

Ein Zugangshindernis kann selbst ausgezeichnete Inhalte unsichtbar machen. Die gegenteilige Reaktion — sämtliche Sicherheit zu entfernen und jedem Bot unbegrenzten Zugang zu geben — ist ebenfalls falsch. Zwecke und Berechtigungen von Crawlern sollten getrennt verwaltet werden.

Nicht verwechseln

- Crawling: eine URL aufrufen und ihren Inhalt anfordern.
- Indexierung: Inhalte zu einem durchsuchbaren Datensatz verarbeiten.
- Abruf: einen passenden Datensatz für eine bestimmte Frage auswählen.
- Training: ein Vorgang der Modellentwicklung; es ist nicht dasselbe wie Crawling.

Was sollten Sie tun?

1. Testen Sie anonymen Zugriff und HTTP-Statuscodes wichtiger URLs.
2. Prüfen Sie robots.txt, Firewall, Ratenbegrenzung und Bot-Verifizierung getrennt.
3. Verwenden Sie für Bot-Namen und Zwecke nur die aktuelle offizielle Anbieterdokumentation.
4. Behandeln Sie Suchzugang und Trainingszugang nicht als dieselbe Richtlinie.
5. Gestalten Sie eine enge Freigabe für verifizierte Bots, statt eine Sicherheitsregel vollständig zu entfernen.

Wie wird es geprüft?

- Liefert die URL den Status 200 zusammen mit dem tatsächlichen Inhalt?
- Was weist robots.txt für den betreffenden User-Agent aus?
- Blockiert CDN oder Sicherheitsschicht einen verifizierten Bot?
- Wurden HTML-, PDF- und JSON-Oberflächen getrennt getestet?
- Wurde das Ergebnis mit Datum, IP- oder Agentenkontext und Antwortinhalt protokolliert?

Grenze

> Crawler-Zugang kann eine notwendige Bedingung sein; er garantiert weder Indexierung, Abruf, Zitierung, Training noch Empfehlung. Bot-Namen und Anbieterrichtlinien können sich ändern.

In einem Satz merken

> Die Tür zu erreichen ist der erste Schritt; eingelassen und ausgewählt zu werden sind andere Schritte.

Quellen: S03, S04, S09, S10

Verwandte Einträge: NGQ-010, NGQ-011, NGQ-017

NGQ-017 — Was ist Indexierung, und warum bedeutet das Crawling einer Seite nicht, dass sie indexiert wird?

Technischer Zugang und Datenkonsistenz · Eintrag NGQ-017 · Version 0.3.1

> **Kürzeste Antwort** Eine Seite zu lesen bedeutet nicht, sie einem Suchdatensatz hinzuzufügen.

Direkte Antwort

Indexierung ist die Analyse abgerufener Inhalte und ihre Umwandlung in einen nutzbaren Datensatz eines Such- oder Abrufsystems. Eine Seite kann crawlbar und dennoch nicht indexiert sein, etwa wegen einer noindex-Anweisung, doppelter Inhalte, geringer Verarbeitbarkeit, einer Qualitätsentscheidung, eines technischen Fehlers oder des Systemumfangs.

Einfach erklärt

Eine Bibliothekarin kann ein Buch entgegennehmen, ohne es in den Katalog aufzunehmen. Das Buch gesehen zu haben bedeutet nicht, dass es eine Katalognummer erhalten hat oder bei einer Suche erscheint.

Warum ist das wichtig?

Wer erfolgreiches Crawling mit erfolgreicher Indexierung gleichsetzt, stellt die falsche Diagnose. Ein Website-Betreiber fügt dann möglicherweise immer neue Inhalte hinzu, ohne zu untersuchen, warum eine zugängliche Seite trotzdem nicht ausgewählt werden kann.

Nicht verwechseln

- Entdeckung, Crawling, Rendering, Indexierung und Abruf sind getrennte Zustände.
- robots.txt steuert den Zugang; noindex ist eine Indexierungsanweisung.
- Ein öffentlicher Suchindex und der private RAG-Index einer Organisation sind nicht dasselbe.

Was sollten Sie tun?

1. Prüfen Sie Indexierbarkeitssignale wichtiger URLs.
2. Betrachten Sie noindex, Canonical, Weiterleitung und HTTP-Status gemeinsam.
3. Kennzeichnen Sie bei doppelten Seiten die bevorzugte kanonische URL eindeutig.
4. Testen Sie, ob per JavaScript erzeugte oder erst nach einem Zugriff sichtbare Inhalte tatsächlich verarbeitet werden können.
5. Wenn ein Anbieter Diagnosewerkzeuge bereitstellt, protokollieren Sie das Ergebnis mit Datum.

Wie wird es geprüft?

- Wurde die Seite gecrawlt oder lediglich entdeckt?

- Gibt es eine noindex-Anweisung oder einen widersprüchlichen Canonical?
- Ist der ausgelieferte Inhalt leer, unvollständig oder an eine Sitzung gebunden?
- Für welches System wurde der Indexstatus gemessen?
- Wurde das Vorhandensein im Index mit dem Abruf für eine bestimmte Anfrage verwechselt?

Grenze

> Der Indexstatus eines Anbieters sagt nichts über den Index eines anderen aus. Indexierung garantiert nicht die Verwendung in einer bestimmten Antwort.

In einem Satz merken

> Crawling führt durch die Tür; Indexierung trägt den Gegenstand in den Katalog ein.

Quellen: S03, S04, S11

Verwandte Einträge: NGQ-010, NGQ-011, NGQ-016, NGQ-019

NGQ-018 — Was sind strukturierte Daten, und wie können sie KI-Systemen helfen, eine Entität richtig zu verstehen?

Technischer Zugang und Datenkonsistenz · Eintrag NGQ-018 · Version 0.3.1

> **Kürzeste Antwort** Strukturierte Daten erläutern Maschinen die Angaben einer Seite in geordneten Feldern.

Direkte Antwort

Strukturierte Daten sind Markup, das Maschinen die Angaben einer Seite mithilfe vordefinierter Felder und Beziehungen erklärt. Sie können Typ, Namen, Verknüpfungen und Merkmale einer Entität klarer machen, verwandeln eine falsche Aussage aber nicht in Wahrheit und garantieren nicht, dass jedes KI-System die Daten nutzt.

Einfach erklärt

Die Beschriftung „zerbrechliche Trinkgläser, 12 Stück“ sagt über einen Karton mehr aus als nur „Gegenstände“. Das Etikett verändert den Inhalt nicht; es beschreibt ihn lediglich geordneter.

Warum ist das wichtig?

Ausdrückliche Felder können Entitätsverwechslungen und mehrdeutige Beziehungen verringern. Sagt das Markup jedoch etwas anderes als die sichtbare Seite, entsteht ein neues Vertrauensproblem.

Nicht verwechseln

- JSON ist ein Datenformat; JSON-LD verwendet JSON und ergänzt die Bedeutung verknüpfter Daten.
- Schema.org ist ein Vokabular; daraus folgt nicht, dass jeder Anbieter jedes Feld verwendet.
- Strukturierte Daten ersetzen sichtbare Inhalte nicht.

Was sollten Sie tun?

1. Berichtigen Sie zuerst die Tatsache im sichtbaren Text.
2. Wählen Sie den richtigen Entitätstyp und eine stabile Kennung.
3. Markieren Sie nur Merkmale, die auf der Seite sichtbar und belegt sind.
4. Stimmen Sie Beziehungen, Namen und URLs mit den übrigen kanonischen Datensätzen ab.
5. Prüfen Sie Syntax und sachliche Richtigkeit getrennt.

Wie wird es geprüft?

- Ist das Markup syntaktisch gültig?
- Ist der Entitätstyp richtig?

- Erscheinen die ausgezeichneten Angaben auch auf der sichtbaren Seite?
- Widersprechen sich kanonische URL und Identitätsverknüpfungen?
- Wurde eine unbelegte Auszeichnung, Bewertung oder Eigentumsaussage hinzugefügt?

Grenze

> Gültiges Markup garantiert weder ein Rich Result, Indexierung, Zitierung, Empfehlung noch eine korrekte KI-Ausgabe.

In einem Satz merken

> Strukturierte Daten beschreiben die Wirklichkeit klarer; sie erschaffen sie nicht.

Quellen: S05, S06, S07, S08

Verwandte Einträge: NGQ-009, NGQ-019, NGQ-020, NGQ-024

NGQ-019 — Warum müssen sichtbares HTML, strukturierte Daten und kanonisches JSON dieselbe Wahrheit ausdrücken?

Technischer Zugang und Datenkonsistenz · Eintrag NGQ-019 · Version 0.3.1

> **Kürzeste Antwort** Menschliche und maschinelle Oberflächen dürfen sich bei derselben Entität nicht widersprechen.

Direkte Antwort

Das von Menschen gelesene HTML, die strukturierten Daten der Seite und das kanonische JSON für Maschinendatensätze dürfen sich bei Identität, Beziehungen, Merkmalen, Grenzen, Daten oder Status einer Entität nicht widersprechen. Die Sätze müssen nicht gleich sein, wohl aber ihre sachliche Bedeutung.

Einfach erklärt

Im Schaufenster steht „24 Stunden geöffnet“, das Kassensystem meldet „Schließt um 18 Uhr“, und auf der offiziellen Infokarte steht „Am Wochenende geschlossen“. Niemand weiß, was stimmt. Alle drei Oberflächen müssen dieselbe Wahrheit ausdrücken.

Warum ist das wichtig?

Widersprüchliche Oberflächen führen Nutzende, Crawler, Prüfende und interne Systeme zu unterschiedlichen Ergebnissen. Falsche Angaben können sich anschließend auf weitere Plattformen ausbreiten.

Nicht verwechseln

- Dieselbe Wahrheit verlangt nicht denselben Satz.
- JSON und JSON-LD müssen nicht dieselbe Aufgabe erfüllen.
- Eine kanonische URL und ein kanonischer Identitätsdatensatz sind verschiedene Konzepte.

Was sollten Sie tun?

1. Bestimmen Sie einen verifizierten Quelldatensatz.
2. Erzeugen Sie HTML, JSON-LD und JSON aus diesem Datensatz oder gleichen Sie sie daran ab.
3. Stimmen Sie Name, Typ, Eigentum, Leistung, geografischen Bezug, Datum und Status ab.
4. Aktualisieren Sie bei einer Änderung alle Oberflächen im selben Versionsereignis.
5. Entfernen oder verschieben Sie alte Kopien, oder kennzeichnen Sie sie als historisch.

Wie wird es geprüft?

- Verwenden alle drei Oberflächen dieselbe Entitätskennung?

- Stimmen Name, Eigentum und Leistungsangaben überein?
- Sind Daten und Gültigkeitsfelder abgestimmt?
- Behaupten die strukturierten Daten mehr als der sichtbare Text?
- Wurden alle Kopien nach der Änderung erneut ausgelesen?

Grenze

> Konsistenz ist für Richtigkeit notwendig, doch dieselbe Unwahrheit auf drei Oberflächen bleibt eine falsche Repräsentation. Auch ihre Beleggrundlage muss verifiziert werden.

In einem Satz merken

> Die drei Oberflächen müssen nicht denselben Satz verwenden; sie müssen dieselbe Wahrheit ausdrücken.

Quellen: S05, S06, S07, S08, S11

Verwandte Einträge: NGQ-018, NGQ-020, NGQ-021

Kanonische Identität und Entitätstrennung

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-020 — Was ist ein kanonischer Identitätsdatensatz, und warum sollte ein Primärdatensatz die Entität bestimmen?

Kanonische Identität und Entitätstrennung · Eintrag NGQ-020 · Version 0.3.1

> **Kürzeste Antwort** Ein primärer Identitätsdatensatz verhindert konkurrierende Wahrheitsversionen über dieselbe Entität.

Direkte Antwort

In NOMOS GEO ist ein kanonischer Identitätsdatensatz der Primärdatensatz, der die stabile Identität, Namen, den Typ, Beziehungen, Gültigkeitsstatus und Belegverknüpfungen einer Entität verwaltet. Ein einziger Primärdatensatz verhindert, dass sich um dieselbe Entität konkurrierende Wahrheitsversionen bilden.

Einfach erklärt

Stellen Sie sich vor, verschiedene Notizbücher nennen für dieselbe Person unterschiedliche Geburtsdaten. Hält jeder sein eigenes Buch für richtig, wächst die Verwirrung. Der Primärdatensatz ist die verlässliche Referenz, mit der andere Kopien abgeglichen werden.

Warum ist das wichtig?

Verstreute Identitätsdatensätze verursachen falsche Zusammenführungen, veraltete Namen, widersprüchliche Eigentumsangaben und unterbrochene Verbindungen zwischen Sprachausgaben. Ein Primärdatensatz erleichtert außerdem die Nachverfolgung von Änderungen.

Nicht verwechseln

- Ein kanonischer Identitätsdatensatz ist nicht die Entität selbst.
- Eine kanonische URL ist ein Präferenzsignal zwischen Webkopien, kein vollständiges Identitätsverwaltungssystem.
- Der Primärdatensatz ersetzt keine unabhängigen externen Belege.

Was sollten Sie tun?

1. Vergeben Sie für jede Entität eine stabile, eindeutige Kennung.
2. Führen Sie kanonische, alternative, frühere und sprachspezifische Namen getrennt.
3. Erfassen Sie Entitätstyp, Beziehungen, Status und Gültigkeitsdaten.
4. Erstellen Sie auf Feldebene Verknüpfungen zu Quellen und Belegen.
5. Verbinden Sie andere Seiten und Datensätze mit dem Primärdatensatz.

Wie wird es geprüft?

- Gibt es konkurrierende Primärdatensätze für dieselbe Entität?
- Wurde die stabile Identität über Versionen hinweg bewahrt?
- Besitzen Änderungen von Namen und Beziehungen einen Verlauf?
- Verweisen externe Kennungen auf die richtige Entität?
- Gibt der Primärdatensatz eine Eigenaussage als unabhängigen Beleg aus?

Grenze

> „Kanonischer Identitätsdatensatz“ ist ein in diesem Werk vorgeschlagenes Governance-Konzept. Es ist kein gemeinsamer offizieller Begriff von ORCID, ROR, DOI oder Schema.org.

In einem Satz merken

> Ein Primärdatensatz pro Entität gibt vielen Oberflächen eine gemeinsame Wahrheitsrichtung.

Quellen: S07, S08, S11, S12, S13, S14

Verwandte Einträge: NGQ-004, NGQ-019, NGQ-021, NGQ-022, NGQ-023

NGQ-021 — Wie sollte sich ein kanonischer Identitätsdatensatz ändern, wenn sich Name, Typ, Eigentümer oder Status einer Entität ändern?

Kanonische Identität und Entitätstrennung · Eintrag NGQ-021 · Version 0.3.1

> **Kürzeste Antwort** Erfassen Sie die Änderung mit Datum, Grund und Beleg, ohne den früheren Zustand zu löschen.

Direkte Antwort

Eine Änderung darf nicht bloß einen alten Wert durch einen neuen ersetzen. Erfassen Sie, was sich geändert hat, warum, zu welchem Zeitpunkt die Änderung wirksam wurde, welchen Beleg es gibt, wer sie genehmigte und auf welche Oberflächen sie übertragen wurde. Behandeln Sie dies als versioniertes Änderungsereignis.

Einfach erklärt

Wechselt ein Haus den Eigentümer, tun Sie nicht so, als habe die alte Urkunde nie existiert. Sie bewahren die Daten des früheren und des aktuellen Zustands sowie den Übertragungsnachweis auf. Ein Identitätsdatensatz soll die Gegenwart zeigen, ohne die Vergangenheit zu löschen.

Warum ist das wichtig?

Ohne Verlauf können eine Korrektur, Umbenennung, Fusion, Schließung oder die Entstehung einer neuen Entität mit einem anderen Ereignis verwechselt werden. Systeme mit älteren Angaben verstehen dann nicht, warum die Änderung erfolgte.

Nicht verwechseln

- Eine Rechtschreibkorrektur und eine Änderung in der realen Welt sind verschieden.
- Eine Namensänderung erzeugt nicht immer eine neue Entität.
- Eine Fusion oder Aufspaltung kann neue Identitätsbeziehungen erfordern und nicht nur die Änderung eines Feldes.

Was sollten Sie tun?

1. Klassifizieren Sie die Art der Änderung.
2. Erfassen Sie früheren und neuen Wert, Wirksamkeitsdatum und Beleg.
3. Entscheiden Sie, ob die stabile Identität fortbesteht.
4. Erstellen Sie eine Verteilungsliste für HTML, strukturierte Daten, JSON und externe Datensätze.
5. Führen Sie nach der Aktualisierung einen Rücklese- und Konflikttest durch.

Wie wird es geprüft?

- Ist der frühere Zustand weiterhin historisch einsehbar?
- Gibt es eine Aufzeichnung, die die Änderung genehmigt und belegt?
- Wurde eine alte Identität fälschlich fortgeführt, obwohl eine neue Entität erforderlich war?
- Wurden alle Oberflächen aktualisiert?
- Gibt es von alter URL und Identität eine richtige Weiterleitung oder Beziehung?

Grenze

> Die Aktualisierung eines technischen Datensatzes erzeugt nicht selbst die rechtliche Wirkung einer Änderung. Rechtsfolgen hängen von befugten Dokumenten, Registern und den Tatsachen des Einzelfalls ab.

In einem Satz merken

> Eine saubere Aktualisierung zeigt das Heute, ohne das Gestern zu leugnen.

Quellen: S14, S15, S19, S20, S22, S35

Verwandte Einträge: NGQ-019, NGQ-020, NGQ-022, NGQ-028, NGQ-029

NGQ-022 — Worin unterscheiden sich kanonischer Name, Alternativname, früherer Name und übersetzter Name?

Kanonische Identität und Entitätstrennung · Eintrag NGQ-022 · Version 0.3.1

> **Kürzeste Antwort** Führen Sie die verschiedenen Namen einer Entität getrennt und versehen Sie sie mit Rolle und Gültigkeitszeitraum.

Direkte Antwort

Ein kanonischer Name ist der bevorzugte Primärname in einem bestimmten Datensatz und Kontext. Ein Alternativname ist ein anderer aktueller Name derselben Entität. Ein früherer Name ist nicht mehr der aktuelle Primärname und wird mit einem Datumsbereich bewahrt. Ein übersetzter Name ist die Form in einer anderen Sprache; er schafft keine neue Entität.

Einfach erklärt

Amtlicher Name, gebräuchlicher Kurzname, früherer Familienname und Schreibweise in einer anderen Sprache gehören in unterschiedliche Felder. Werden alle in ein einziges Namensfeld geschrieben, weiß niemand, welcher Name wo und wann zu verwenden ist.

Warum ist das wichtig?

Ohne Namenstypen kann ein früherer Name als aktuell behandelt, können zwei Entitäten falsch zusammengeführt oder die Sprachseiten einer Entität als unverbunden erkannt werden.

Nicht verwechseln

- Ein kanonischer Name ist nicht zwangsläufig ein universeller Name für jedes Land und jeden Rechtskontext.
- Ein Alternativname kann aktuell sein; ein früherer Name ist historisch.
- Übersetzung und Transliteration sind verschiedene Vorgänge.

Was sollten Sie tun?

1. Erfassen Sie Typ, Sprache und Schrift jedes Namens.
2. Versehen Sie frühere Namen mit Anfangs- und Enddatum.
3. Trennen Sie den rechtlichen Namen von dem Namen, der Nutzenden angezeigt wird.
4. Verwenden Sie gültige BCP-47-Formate für Sprachkennzeichnungen.
5. Verknüpfen Sie jeden Namen mit derselben stabilen Entitätsidentität.

Wie wird es geprüft?

- Sind die Namenstypen ausdrücklich angegeben?

- Wird ein früherer Name als aktuell angezeigt?
- Stimmen Sprach- und Schriftkennzeichnungen?
- Hat eine Übersetzung einen neuen Entitätsdatensatz erzeugt?
- Wurde im Rechtskontext der falsche Name verwendet?

Grenze

> Die Wahl des kanonischen Namens hängt vom Kontext ab. Für Marken-, Unternehmens- und Personennamen können besondere Rechtsregeln gelten.

In einem Satz merken

> Jeder Name kann auf dieselbe Entität verweisen, aber nicht jeder Name erfüllt denselben Zweck.

Quellen: S08, S12, S13, S14, S16

Verwandte Einträge: NGQ-020, NGQ-021, NGQ-023, NGQ-024

NGQ-023 — Wie sollten verschiedene Entitäten mit demselben oder einem ähnlichen Namen unterschieden werden?

Kanonische Identität und Entitätstrennung · Eintrag NGQ-023 · Version 0.3.1

> **Kürzeste Antwort** Verlassen Sie sich nicht allein auf den Namen; prüfen Sie gemeinsam Typ, Identität, Ort, Beziehungen und Zeit.

Direkte Antwort

Entitäten mit gleichen oder ähnlichen Namen dürfen nicht allein aufgrund des Namens zusammengeführt werden. Lösen Sie jede Entität getrennt auf, indem Sie stabile Kennungen, Entitätstyp, rechtlichen Namen, geografischen Bezug, Eigentum, Beziehungen, Daten und verlässliche Quellen kombinieren.

Einfach erklärt

In einer Schule können zwei Schüler „Ahmet Yılmaz“ heißen. Eine Lehrkraft verlässt sich nicht nur auf den Namen, sondern verwendet Klasse, Schülernummer und Geburtsdatum, um die richtige Person zu finden.

Warum ist das wichtig?

Eine falsche Zusammenführung kann die Auszeichnung eines Unternehmens einem anderen oder die Rolle einer Person jemand anderem zuordnen. Eine falsche Trennung zerlegt dieselbe Entität in mehrere Fragmente und verstreut ihre Belege.

Nicht verwechseln

- Falsche Zusammenführung: verschiedene Entitäten als eine behandeln.
- Falsche Trennung: eine Entität als mehrere behandeln.
- Entitätsverknüpfung: einen Datensatz mit der richtigen kanonischen Entität verbinden.

Was sollten Sie tun?

1. Verwenden Sie neben dem Namen mehrere unterscheidende Merkmale.
2. Erfassen Sie eine stabile interne Kennung und geeignete externe Kennungen.
3. Trennen Sie die Typen Marke, Unternehmen, Person, Produkt und Ort.
4. Verschieben Sie bei verbleibender Unsicherheit die Zusammenführung und erfassen Sie einen Konfidenzwert.
5. Verwalten Sie Korrekturen falscher Zuordnungen mit datiertem Verlauf.

Wie wird es geprüft?

- Beruht die Zuordnung nur auf dem Namen?
- Stimmen Typ, Land, Eigentum und Beziehungsdaten überein?
- Gehört die externe Kennung wirklich zu derselben Entität?
- Wurden widersprüchliche Belege ignoriert?
- Besitzt die Zusammenführungsentscheidung einen Konfidenzwert und eine Begründung?

Grenze

> Keine einzelne Kennung ist in jedem Kontext unfehlbar. Entitätsauflösung benötigt mehrere Signale und aktuelle Belege.

In einem Satz merken

> Derselbe Name beweist nicht dieselbe Entität; ein anderer Name beweist nicht zwangsläufig eine andere Entität.

Quellen: S08, S12, S13, S17

Verwandte Einträge: NGQ-004, NGQ-020, NGQ-022, NGQ-024

NGQ-024 — Warum sollten Marke, Unternehmen, Produkt, Dienstleistung und Gründer als getrennte Entitäten erfasst werden?

Kanonische Identität und Entitätstrennung · Eintrag NGQ-024 · Version 0.3.1

> **Kürzeste Antwort** Marke, Unternehmen, Produkt, Dienstleistung und Gründer können verbunden sein; identisch sind sie nicht.

Direkte Antwort

Eine Marke, ein rechtliches Unternehmen, ein Produkt, eine Dienstleistung und ein Gründer haben unterschiedliche Merkmale, Eigentumsbeziehungen, Belege und Lebenszyklen. Ihre Beziehungen sollten erfasst werden, doch sie dürfen nicht so zusammengeführt werden, als wären sie eine einzige Entität.

Einfach erklärt

Bei einem Restaurant ist das Schild die Marke, die Organisation mit der Betriebserlaubnis das Unternehmen, ein Gericht auf der Karte ein Produkt, die Lieferung nach Hause eine Dienstleistung und die Person, die das Geschäft gegründet hat, der Gründer. Sie hängen zusammen, sind aber nicht dasselbe.

Warum ist das wichtig?

Wer diese Identitäten vermischt, kann persönliches Eigentum eines Gründers dem Unternehmen, eine Produktauszeichnung jeder Dienstleistung der Marke oder das Eigentum einem Betreiber zuschreiben, dem die Marke nicht gehört.

Nicht verwechseln

- Eine Marke und eine eingetragene Handelsmarke sind nicht dasselbe Konzept.
- Der Unternehmensname muss nicht mit dem Markennamen übereinstimmen.
- Ein Produkt kann ein körperliches oder lizenzierbares Angebot sein; eine Dienstleistung kann eine Tätigkeit sein.
- Gründer zu sein bedeutet nicht, aktueller Eigentümer oder Geschäftsführer zu sein.

Was sollten Sie tun?

1. Erstellen Sie für jeden Entitätstyp eine eigene stabile Identität.
2. Erfassen Sie Eigentum, Betrieb, Herstellung, Erbringung und Gründung als getrennte Beziehungen.
3. Erfassen Sie Datum und Beleg jeder Beziehung.
4. Verwenden Sie auf Webseiten und in strukturierten Daten den richtigen Typ.
5. Übertragen Sie ein Merkmal nicht automatisch von einer Entität auf eine verbundene Entität.

Wie wird es geprüft?

- Wurde die Marke als rechtliches Unternehmen dargestellt?
- Wurde der Erfolg eines Produkts auf das gesamte Unternehmen übertragen?
- Wurde der Gründer als aktuell befugte Person behandelt?
- Wurden Eigentum und Betrieb getrennt?
- Besitzt jede Entität eigene Quellen und Gültigkeitsdaten?

Grenze

> Getrennte Datensätze dienen der richtigen Modellierung von Beziehungen, nicht ihrer Auflösung. Der rechtliche Status von Marke und Unternehmen ist anhand der einschlägigen Register und des nationalen Rechts zu beurteilen.

In einem Satz merken

> Verbunden zu sein bedeutet nicht, identisch zu sein.

Quellen: S08, S18, S19, S20

Verwandte Einträge: NGQ-004, NGQ-020, NGQ-023, NGQ-025

Rollen, Befugnisse und Lebenszyklus

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-025 — Worin unterscheiden sich Gründer, Eigentümer, Geschäftsleiter, Beschäftigter, gesetzlicher Vertreter und Zeichnungsberechtigter?

Rollen, Befugnisse und Lebenszyklus · Eintrag NGQ-025 · Version 0.3.1

> **Kürzeste Antwort** Die Rolle einer Person bestimmt nicht automatisch jede Befugnis, die sie besitzt.

Direkte Antwort

Ein Gründer wirkt an der Errichtung einer Organisation mit; ein Eigentümer hält Eigentum oder eine Beteiligung; ein Geschäftsleiter hat Leitungs- und Entscheidungsaufgaben; ein Beschäftigter arbeitet in einem Arbeitsverhältnis; ein gesetzlicher Vertreter handelt aufgrund einer bestimmten Vertretungsmacht; und ein Zeichnungsberechtigter darf innerhalb eines festgelegten Umfangs für die Organisation unterzeichnen. Eine Person kann mehrere Rollen innehaben, doch keine dieser Rollen erzeugt automatisch eine andere.

Einfach erklärt

Denken Sie an ein Theater. Wer es ins Leben gerufen hat, kann der Gründer sein. Einer anderen Person gehört vielleicht das Gebäude, eine weitere leitet den Betrieb, die Darstellenden sind Beschäftigte, ein Vertreter verhandelt Verträge und ein Zeichnungsberechtigter unterschreibt sie. Eine Person kann mehrere dieser Aufgaben übernehmen, doch sie bedeuten nicht dasselbe.

Warum ist das wichtig?

Wer Rollen verwechselt, ordnet Befugnis, Verantwortlichkeit und Repräsentation falsch zu. Die Bezeichnung „Gründer“ gibt einer Person für sich allein kein aktuelles Recht, einen Vertrag für das Unternehmen zu unterschreiben.

Nicht verwechseln

- Eigentum ist ein wirtschaftliches oder rechtliches Interesse; Leitung ist eine Funktion mit bestimmten Pflichten und Befugnissen.
- Ein Arbeitsverhältnis verleiht nicht automatisch Vertretungsmacht für die Organisation.
- Rechtliche Vertretungsmacht und die Befugnis zur Unterzeichnung eines bestimmten Dokuments können sich in Umfang und Beleggrundlage unterscheiden.

Was sollten Sie tun?

1. Verwalten Sie jede Rolle als eigenen Datensatz mit Anfangs- und Enddatum.
2. Verknüpfen Sie die Rolle mit der Entscheidung, dem Vertrag, Registereintrag oder der Vollmacht, auf der sie beruht.
3. Speichern Sie Rolle und Befugnisumfang in getrennten Feldern.

4. Prüfen Sie beim Ausscheiden einer Person jede mit ihr verbundene Befugnis einzeln.
5. Unterscheiden Sie in Web- und Maschinendatensätzen zwischen aktueller und früherer Rolle.

Wie wird es geprüft?

- Ist klar, welche Rolle die Person in welchem Zeitraum innehatte?
- Sind Grundlage der Rolle und befugendes Organ benannt?
- Wurde ein Eigentümer oder Gründer automatisch als Zeichnungsberechtigter behandelt?
- Wird eine beendete Rolle noch als aktuell dargestellt?
- Wurden aus einer einzigen Rollenbezeichnung mehrere Befugnisse abgeleitet?

Grenze

> Dieser Eintrag bietet eine allgemeine Abgrenzung. Die Rechtsfolgen von Vertretung, Leitung und Zeichnungsbefugnis für eine konkrete Organisationsform sind anhand des geltenden Rechts, offizieller Register und der Organisationsdokumente zu prüfen.

In einem Satz merken

> Ihre Rolle beschreibt, wer Sie sind; Ihre Befugnis beschreibt, was Sie tun dürfen.

Quellen: S19, S20, S21, S22

Verwandte Einträge: NGQ-024, NGQ-026, NGQ-027, NGQ-028

NGQ-026 — Wie sollten Einzel-, Gesamt-, beschränkte und auf Vollmacht beruhende Zeichnungsbefugnis unterschieden werden?

Rollen, Befugnisse und Lebenszyklus · Eintrag NGQ-026 · Version 0.3.1

> **Kürzeste Antwort** Eine Zeichnungsbefugnis muss fünf Fragen beantworten: Wer darf was, wie, wann und auf welcher Grundlage unterschreiben?

Direkte Antwort

Bei Einzelbefugnis kann eine Person innerhalb des festgelegten Umfangs allein unterzeichnen. Bei Gesamtbefugnis müssen die erforderlichen Personen gemeinsam handeln. Eine beschränkte Befugnis ist nach Betrag, Geschäft, Ort, Zeit oder Gegenstand begrenzt. Eine auf Vollmacht beruhende Befugnis leitet sich aus der gültigen und übertragbaren Befugnis des Vollmachtgebers ab und bleibt innerhalb der in der Vollmacht genannten Grenzen.

Einfach erklärt

Stellen Sie sich einen Tresor vor. Öffnet ihn ein Schlüssel, gleicht das Einzelbefugnis. Sind zwei Schlüssel gleichzeitig nötig, gleicht das Gesamtbefugnis. Öffnet ein Schlüssel nur eine Schublade, ist die Befugnis beschränkt. Hat Ihnen jemand den Schlüssel für einen bestimmten Zweck und Zeitraum überlassen, ähnelt dies einer Vollmacht.

Warum ist das wichtig?

Die Bezeichnung „zeichnungsberechtigt“ allein sagt nicht, welches Geschäft, bis zu welchem Betrag, an welchem Datum und mit wie vielen Unterschriften abgeschlossen werden darf.

Nicht verwechseln

- Zeichnungsweise und Befugnisumfang sind verschiedene Fragen.
- Allein unterzeichnen zu dürfen bedeutet keine unbegrenzte Befugnis.
- Eine Vollmacht gestattet dem Bevollmächtigten nicht jedes denkbare Geschäft.

Was sollten Sie tun?

1. Erfassen Sie die betroffene Organisation und die Befugnisquelle ausdrücklich.
2. Speichern Sie Zeichnungsweise, Umfang, Betrag, Dauer und Gebiet in getrennten Feldern.
3. Drücken Sie bei Gesamtbefugnis die erforderliche Kombination maschinenprüfbar aus.
4. Prüfen Sie gesondert, ob der Vollmachtgeber die betreffende Befugnis besaß und übertragen durfte.
5. Verfolgen Sie Ablauf, Widerruf und gegebenenfalls den Registerstatus.

Wie wird es geprüft?

- Fällt das Geschäft in den angegebenen Umfang?
- Ist die erforderliche Unterschriftenkombination vollständig?
- War die Befugnis am Tag des Geschäfts gültig?
- Wurden Delegationskette und Recht zur Übertragung geprüft?
- Wurden Registrierungserfordernisse oder Wirkungen gegenüber Dritten beurteilt?

Grenze

> Die rechtliche Wirksamkeit einer Zeichnungsbefugnis hängt von Organisationsform, Urkunde, Register, Geschäft und anwendbarem Recht ab. Dieser Eintrag ist keine Rechtsberatung für einen Einzelfall.

In einem Satz merken

> Wer unterzeichnen darf, ist zusammen mit dem Was, Wie, Wann und der Grundlage zu beantworten.

Quellen: S19, S21, S22, S23

Verwandte Einträge: NGQ-025, NGQ-027, NGQ-028, NGQ-032

NGQ-027 — Wie sind Belege aus Handelsregister, Organbeschluss, Unterschriftserklärung, Vollmacht und Systemberechtigung aufeinander zu beziehen?

Rollen, Befugnisse und Lebenszyklus · Eintrag NGQ-027 · Version 0.3.1

> **Kürzeste Antwort** Kein einzelnes Dokument beantwortet jede Befugnisfrage; die Datensätze müssen gemeinsam gelesen werden.

Direkte Antwort

Diese Datensätze lassen sich nicht auf einer einfachen Skala von „stärkster“ zu „schwächster“ Beleg einordnen, weil sie verschiedene Fragen beantworten. Ein Handelsregister zeigt eingetragene Tatsachen; ein Organbeschluss hält den institutionellen Willen fest; eine Unterschriftserklärung liefert eine Unterschriftsprobe; eine Vollmacht bestimmt den übertragenen Umfang; und eine Systemberechtigung zeigt technischen Zugang. Der richtige Beleg hängt von der behaupteten Befugnis und dem Geschäftsdatum ab; häufig sind mehrere Datensätze gemeinsam zu betrachten.

Einfach erklärt

Eine Zugangskarte kann einer Person die Tür zu einem Gebäude öffnen. Das beweist nicht, dass sie das Gebäude verkaufen darf. Die Karte belegt technischen Zugang; ein offizieller Beschluss oder eine Vollmacht belegt eine andere Art von Befugnis.

Warum ist das wichtig?

Schwere Fehler entstehen, wenn technischer Zugang als rechtliche Befugnis, eine Unterschriftsprobe als aktuelle Befugnis oder ein alter Organbeschluss als Beleg der gegenwärtigen Registerlage behandelt wird.

Nicht verwechseln

- Echtheit eines Dokuments und seine Eignung für eine konkrete Aussage sind verschiedene Fragen.
- Technische Berechtigung ist keine rechtliche Befugnis.
- Eine Unterschriftsprobe allein belegt keine Befugnis für den Umfang eines Geschäfts.
- Die Wirkung einer Eintragung, eines Beschlusses oder einer Vollmacht hängt vom Rechtskontext ab.

Was sollten Sie tun?

1. Schreiben Sie den genau zu belegenden Satz und das maßgebliche Geschäftsdatum auf.
2. Bestimmen Sie, welche Frage jeder Beleg beantworten kann.
3. Prüfen Sie ausstellende Stelle, Version und Gültigkeit jedes Dokuments.

4. Lassen Sie bei Widersprüchen Aktualität und Rechtswirkung von einer qualifizierten Fachperson beurteilen.
5. Führen Sie technische Zugangsdatensätze getrennt von Nachweisen rechtlicher Befugnis.

Wie wird es geprüft?

- Betrifft das Dokument die richtige Person und Organisation?
- War es am Tag des Geschäfts gültig?
- Stützt es die betreffende Geschäftsart und den betreffenden Wert?
- Gibt es einen Widerruf oder einen neueren Beschluss?
- Gewährt das technische System mehr Zugang, als die dokumentierte Befugnis erlaubt?

Grenze

> Die Belegzuordnung nach NOMOS entscheidet nicht über Rechtswirksamkeit. Widersprüchliche Datensätze und folgenreiche Geschäfte sollten durch eine befugte juristische Fachperson anhand offizieller Unterlagen beurteilt werden.

In einem Satz merken

> Der stärkste Beleg beantwortet nicht jede Frage, sondern stützt den richtigen Satz zum richtigen Zeitpunkt.

Quellen: S19, S20, S21, S22, S23

Verwandte Einträge: NGQ-007, NGQ-025, NGQ-026, NGQ-028

NGQ-028 — Wie muss jeder Datensatz aktualisiert werden, wenn sich eine Rolle oder Zeichnungsbefugnis ändert, endet oder widerrufen wird?

Rollen, Befugnisse und Lebenszyklus · Eintrag NGQ-028 · Version 0.3.1

> **Kürzeste Antwort** Endet eine Rolle, muss jeder damit verbundene physische und digitale Zugangsweg geprüft werden.

Direkte Antwort

Eine Rolle oder Befugnis zu ändern bedeutet nicht, lediglich einen Namen aus einer Liste zu löschen. Das Änderungsereignis muss erfasst und kontrolliert an jedes betroffene Ziel verteilt werden, darunter Identitätssysteme, Personal- und Rechtsunterlagen, Zeichnungsmatrizen, Zugangssysteme, API-Schlüssel, Geräte, Agenten, Webseiten und maschinenlesbare Datensätze.

Einfach erklärt

Wenn Sie beim Ausscheiden eines Beschäftigten den Ausweis für das Hauptgebäude sperren, aber Lagerschlüssel, E-Mail-Konto und Fernzugang aktiv lassen, ist der Vorgang nicht abgeschlossen. Jede Tür muss einzeln geprüft werden.

Warum ist das wichtig?

Unvollständiges Offboarding hinterlässt Restzugänge, unbefugte Repräsentation, veraltete Webangaben und herrenlose Konten. Der zentrale Datensatz kann aktuell aussehen, während reale Systeme die alte Befugnis weiter anerkennen.

Nicht verwechseln

- Eine Rolle zu beenden und jeden Zugangsweg zu schließen sind nicht dasselbe Ereignis.
- Aussetzung, Widerruf und Ablauf sind unterschiedliche Zustände.
- Einen Datensatz zu ändern und die Änderung im Zielsystem umzusetzen sind verschiedene Schritte.

Was sollten Sie tun?

1. Erfassen Sie Kennung, Art, Zeitpunkt, Grund und Genehmigung der Änderung.
2. Ermitteln Sie mithilfe des Inventars jedes betroffene System und jede Publikationsoberfläche.
3. Schließen Sie zuerst die Zugangswege mit hohem Risiko.
4. Prüfen Sie Token, Schlüssel, Sitzungen, Gruppenmitgliedschaften und Agentendelegationen getrennt.
5. Sammeln Sie für jedes Ziel Anwendungs- und Rücklesenachweise.
6. Löschen Sie keine Aufzeichnungen, die für historische Verantwortlichkeit benötigt werden.

Wie wird es geprüft?

- Hat die Änderung jedes Ziel erreicht?
- Funktioniert eine alte Sitzung oder ein alter Authentifikator weiterhin?
- Zeigen Web- und Maschinendatensätze die aktuelle Rolle?
- Sind Dienst- oder Agentenkonten nun ohne Verantwortlichen?
- Ist die Schließungsentscheidung belegt?

Grenze

> Löschen ist nicht immer die richtige Reaktion. Aktive Befugnis muss enden, während historische Protokolle, gesetzliche Aufbewahrungspflichten und Prüfbelege erhalten bleiben.

In einem Satz merken

> Wenn eine Rolle endet, schließen Sie jede von ihr geöffnete Tür — nicht nur den Namen in einer Liste.

Quellen: S22, S24, S25, S26, S27, S28

Verwandte Einträge: NGQ-021, NGQ-025, NGQ-026, NGQ-029, NGQ-030

NGQ-029 — Wie kann eine Organisation nachweisen, dass eine Rollen- oder Befugnisänderung tatsächlich jedes System erreicht hat?

Rollen, Befugnisse und Lebenszyklus · Eintrag NGQ-029 · Version 0.3.1

> **Kürzeste Antwort** Lesen Sie den neuen Zustand in jedem System aus und testen Sie anschließend getrennt, dass der alte Zugang nicht mehr funktioniert.

Direkte Antwort

Die Verteilung lässt sich nicht durch eine einzelne Meldung „Vorgang erfolgreich“ belegen. Erfassen Sie für jedes Zielsystem Änderungsauftrag, Empfang, Anwendungsergebnis, Rücklesen des Endzustands, einen Negativtest des früheren Zugangswegs und die Lösung jeder Abweichung.

Einfach erklärt

Zehn Personen eine neue Adresse mitzuteilen beweist nicht, dass alle zehn ihr Adressbuch aktualisiert haben. Sie müssen zusätzlich prüfen, ob jede Nachricht ankam, umgesetzt wurde und die alte Adresse nicht länger verwendet wird.

Warum ist das wichtig?

Ein zentrales System kann aktuell erscheinen, während eine verbundene Anwendung, ein Cache, Token oder externes Konto die frühere Befugnis weiter anerkennt. Diese verborgene Abweichung zählt zu den gefährlichsten Formen von Restzugang.

Nicht verwechseln

- Gesendet: Die Änderung wurde an das Ziel übermittelt.
- Empfangen: Das Ziel hat den Auftrag angenommen.
- Angewendet: Das Ziel hat seinen Zustand geändert.
- Verifiziert: Der neue Zustand wurde zurückgelesen und der alte Zugangsweg getestet.

Was sollten Sie tun?

1. Vergeben Sie für jede Änderung eine eindeutige Ereigniskennung.
2. Erstellen Sie ein Zielsysteminventar und bestimmen Sie den erwarteten Endzustand.
3. Erfassen Sie Zustell-, Anwendungs- und Rücklesenachweise getrennt.
4. Führen Sie einen kontrollierten Negativtest gegen den alten Zugangsweg durch.
5. Wiederholen Sie fehlgeschlagene Ziele und legen Sie ungelöste Fälle Menschen zur Prüfung vor.
6. Schließen Sie das Ereignis erst, wenn jedes Ziel belegt ist.

Wie wird es geprüft?

- Ist die Zielliste vollständig?
- Stimmen erwarteter und beobachteter Zustand in jedem Ziel überein?
- Beruht der Erfolg nur auf dem Protokoll des Senders?
- Wird der Zugang mit altem Token oder alter Sitzung verweigert?
- Sind alle Belege mit derselben Ereigniskennung und Zeitleiste verbunden?

Grenze

> Eine absolute, sofortige Synchronisierung ist in verteilten Systemen nicht immer möglich. Zulässige Verzögerung, Wiederholungsregel und Abschlussregel sollten deshalb im Voraus feststehen.

In einem Satz merken

> Die Änderung zu senden genügt nicht; beobachten Sie den neuen Zustand und belegen Sie, dass der alte Weg geschlossen ist.

Quellen: S27, S28, S35, S36, S37

Verwandte Einträge: NGQ-015, NGQ-021, NGQ-028, NGQ-030, NGQ-033

NGQ-030 — Was sind ein herrenloses Konto, eine Schattenberechtigung, ein Restzugang und ein Authentifikator ohne Verantwortlichen, und wie werden sie erkannt?

Rollen, Befugnisse und Lebenszyklus · Eintrag NGQ-030 · Version 0.3.1

> **Kürzeste Antwort** Zugang ohne bekannten Verantwortlichen, Zweck oder aktuellen Bedarf ist nicht sicher.

Direkte Antwort

Ein herrenloses Konto hat keinen aktuell verantwortlichen Besitzer. Eine Schattenberechtigung ist eine wirksame Berechtigung, die im formalen Datensatz nicht erscheint. Restzugang besteht fort, nachdem Aufgabe oder Bedarf geendet haben. Ein Authentifikator ohne Verantwortlichen ist ein Schlüssel, Token, Gerät oder ähnlicher Mechanismus, der noch funktioniert, obwohl es keinen gültigen Besitzer oder Sponsor mehr gibt.

Einfach erklärt

Ein aktives Benutzerkonto eines ehemaligen Beschäftigten kann herrenlos sein. Eine verborgene, über eine Gruppe geerbte Berechtigung ist eine Schattenberechtigung. Ordnerzugang nach Projektende ist Restzugang. Ein funktionierender API-Schlüssel, für den niemand verantwortlich ist, ist ein Authentifikator ohne Verantwortlichen.

Warum ist das wichtig?

Diese vier Zustände fehlen möglicherweise in gewöhnlichen Listen. Sie eröffnen Möglichkeiten für Angriffe und Fehlhandlungen und machen unklar, wer verantwortlich ist.

Nicht verwechseln

- Konto, Berechtigung, Zugangsweg und Authentifikator sind getrennte Objekte.
- Ein Konto kann einen Besitzer haben und dennoch eine Schattenberechtigung tragen.
- Eine Person kann weiter beschäftigt sein und trotzdem Zugang besitzen, der für ihre aktuelle Rolle nicht mehr nötig ist.

Was sollten Sie tun?

1. Inventarisieren Sie jede menschliche, Dienst-, Anwendungs- und Agentenidentität.
2. Ordnen Sie jeder Identität einen Besitzer, Sponsor, Zweck und Prüftermin zu.
3. Berechnen Sie die effektive Befugnis aus direkten Berechtigungen und Gruppenmitgliedschaften.
4. Prüfen Sie lange ungenutzte Token, Schlüssel und Konten.
5. Gleichen Sie Personal-, Register- und Systemdatensätze ab.

6. Ermitteln Sie vor einer Deaktivierung Abhängigkeiten und erstellen Sie einen kontrollierten Wiederherstellungsplan.

Wie wird es geprüft?

- Gibt es ein Konto ohne Besitzer oder Sponsor?
- Entsteht Befugnis über einen Weg, der im formalen Rollendatensatz fehlt?
- Besteht Zugang nach Ende der Aufgabe oder des Vertrags fort?
- Gibt es einen gemeinsam verwendeten Authentifikator oder einen mit unbekannter Kontrolle?
- Sind letzte Nutzung, Zweck und Prüftermin erfasst?

Grenze

> Nicht jedes ungenutzte Konto ist böswillig. Lässt sich sein Besitzer, Zweck oder fortbestehender Bedarf jedoch nicht belegen, ist es als Risiko zu behandeln.

In einem Satz merken

> Lassen Sie keinen Zugang offen, dessen Besitzer, Zweck und aktueller Bedarf nicht belegt werden können.

Quellen: S24, S25, S26, S27, S28, S29, S30

Verwandte Einträge: NGQ-028, NGQ-029, NGQ-031, NGQ-032

Maschinenidentität und Agentenverantwortung

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-031 — Warum sollten menschliche Konten, Dienstkonten, Service Principals, verwaltete Identitäten und KI-Agentenidentitäten getrennt verwaltet werden?

Maschinenidentität und Agentenverantwortung · Eintrag NGQ-031 · Version 0.3.1

> **Kürzeste Antwort** Unterschiedliche Akteure benötigen getrennte Identitäten; sonst bleibt unklar, wer was getan hat.

Direkte Antwort

Diese Identitätstypen stehen für unterschiedliche Akteure, Lebenszyklen und Risiken. Ein menschliches Konto gehört zu einer Person; ein Dienstkonto zu einer nichtmenschlichen Arbeitslast; ein Service Principal repräsentiert eine Anwendungsinstanz; eine verwaltete Identität ist eine vom Cloud-Anbieter verwaltete Arbeitslastidentität; und eine KI-Agentenidentität gehört zu einem Agenten, dessen Zweck, Sponsor, Werkzeuge und Handlungen gesondert verfolgt werden müssen.

Einfach erklärt

In einem Betrieb sollten Mitarbeiterausweis, Berechtigung einer automatischen Türsteuerung und Identität eines Lieferroboters nicht derselbe Ausweis sein. Jeder Akteur muss einzeln erkannt werden, damit er passende Berechtigungen erhält und seine Handlungen richtig zugeordnet werden können.

Warum ist das wichtig?

Automatisierung über ein menschliches Konto verschleiert Verantwortlichkeit, trägt häufig zu weitreichende Befugnisse und kann ausfallen, wenn die Person ausscheidet. Einen Agenten nur durch einen Modellnamen zu kennzeichnen zeigt außerdem nicht, welche konkrete Agenteninstanz gehandelt hat.

Nicht verwechseln

- Identität, Authentifikator und Berechtigung sind nicht dasselbe.
- Anwendungsobjekt und Service Principal sind nicht dasselbe Objekt.
- Eine verwaltete Identität ist eine verwaltete Identitätsform; ihre Beziehung zur nutzenden Ressource muss dennoch verfolgt werden.
- Ein KI-Agent ist nicht das zugrunde liegende Modell selbst.

Was sollten Sie tun?

1. Verwenden Sie für jede Arbeitslast und jeden folgenreichen Agenten eine eigene Identität.
2. Betreiben Sie Hintergrundautomatisierung nicht über ein menschliches Konto.
3. Verknüpfen Sie jede Identität mit Zweck, Besitzer oder Sponsor, Umgebung und Lebenszyklus.

4. Bevorzugen Sie, soweit passend, kurzlebige oder verwaltete Zugangsdaten gegenüber langlebigen statischen Geheimnissen.
5. Erfassen Sie Werkzeug-, Modell-, Laufzeit- und Agentenidentitäten getrennt.
6. Wenden Sie das Prinzip der geringsten Rechte an und prüfen Sie Zugänge regelmäßig.

Wie wird es geprüft?

- Ist die Identität richtig klassifiziert?
- Verwendet eine nichtmenschliche Arbeitslast ein menschliches Konto?
- Sind Besitzer oder Sponsor aktuell?
- Wird unnötig ein statischer Schlüssel verwendet?
- Lassen sich die Beziehungen zwischen Agent, Modell, Werkzeugen und Laufzeit nachverfolgen?
- Werden beim Schließen der Identität auch ihre Berechtigungen und Geheimnisse geschlossen?

Grenze

> Anbieter verwenden unterschiedliche Begriffe. NOMOS schlägt ein gemeinsames Prüfvokabular vor; es führt die Identitätsmodelle von Microsoft, Google und AWS nicht zu einem einzigen technischen Schema zusammen.

In einem Satz merken

> Teilen Person, Anwendung, Arbeitslast und Agent eine Identität, lässt sich schwer erkennen, wer was getan hat.

Quellen: S24, S25, S29, S30, S31, S32

Verwandte Einträge: NGQ-030, NGQ-032, NGQ-033

NGQ-032 — Wie ist zu unterscheiden, ob ein KI-Agent für sich selbst, für eine Person oder für eine Organisation handelt?

Maschinenidentität und Agentenverantwortung · Eintrag NGQ-032 · Version 0.3.1

> **Kürzeste Antwort** Erfassen Sie getrennt, wer gehandelt hat, in wessen Namen die Handlung erfolgte und wer für das Ergebnis verantwortlich ist.

Direkte Antwort

Handelt ein Agent über seine eigene Identität, ist er der technische Akteur. Handelt er für eine Person, muss auch deren aktuelle und begrenzte Delegation sichtbar sein. Handelt er für eine Organisation, muss ein Befugnisdatensatz Zweck, Umfang, Werkzeuge, Dauer und Genehmigungsgrenzen der Organisation festlegen. Ausführender, repräsentiertes Subjekt und verantwortliche Partei können bei derselben Handlung verschieden sein.

Einfach erklärt

Ein Assistent kann einen E-Mail-Entwurf vorbereiten, ihn in Ihrem Namen senden oder eine genehmigte Mitteilung über die Supportadresse des Unternehmens versenden. In allen drei Fällen führt der Assistent die Arbeit aus; die genutzte Befugnis und die daraus folgende Verantwortlichkeit sind jedoch nicht gleich.

Warum ist das wichtig?

Die Verwechslung des Akteurs mit der repräsentierten Person erzeugt eine falsche menschliche Urheberschaft, unbegrenzte Delegation und eine Möglichkeit, organisatorische Verantwortung hinter einem Agenten zu verbergen.

Nicht verwechseln

- Technischer Akteur: die Identität, die die Handlung im System ausführt.
- Repräsentiertes Subjekt: die Person oder Organisation, in deren Namen gehandelt wird.
- Befugnisgeber: die Partei, die Delegation oder Organisationsauftrag festlegt.
- Verantwortliche Partei: die Partei, die organisatorische oder rechtliche Verantwortung für das Ergebnis trägt.

Was sollten Sie tun?

1. Erfassen Sie bei jeder Handlung Akteur, Subjekt, Organisation, Initiator, Genehmigenden und verantwortliche Partei getrennt.
2. Bestimmen Sie Umfang, Ziel, Werkzeuge, Dauer und Widerrufsbedingungen der Delegation.
3. Befugen Sie Entwurf, Versand, Unterzeichnung und Zahlung als getrennte Handlungen.

4. Verhindern Sie, dass ein Agent seine eigene Befugnis erweitert.
5. Geben Sie in einer Multi-Agenten-Kette jedem Unteragenten nur die benötigte Befugnis.
6. Erklären Sie externen Nutzenden die KI-Interaktion und den Organisationsstatus des Agenten ohne Irreführung.

Wie wird es geprüft?

- Unterscheidet Token oder Protokoll zwischen Akteur und Subjekt?
- War die Person berechtigt, die Befugnis zu erteilen?
- Bleibt die Handlung innerhalb von Umfang und Dauer der Delegation?
- Gibt es einen Organisationsauftrag und einen menschlichen Sponsor?
- Hat der Agent Entwurfsbefugnis wie Versandbefugnis verwendet?
- Wurde die Identität des Agenten oder der Organisation gegenüber Nutzenden irreführend dargestellt?

Grenze

> Ein technisches Token kann einen Zugangsweg zeigen; allein beweist es keine rechtliche oder organisatorische Befugnis für die Handlung. Ein KI-Agent wird nicht dadurch zur Rechtsperson, dass er eine eigene technische Identität besitzt.

In einem Satz merken

> Erfassen Sie getrennt, wer handelte, in wessen Namen und wer für das Ergebnis verantwortlich ist.

Quellen: S23, S29, S30, S31, S32, S33, S34

Verwandte Einträge: NGQ-025, NGQ-026, NGQ-030, NGQ-031, NGQ-033

NGQ-033 — Wie sollte eine Organisation nachweisen, wer eine Handlung eines KI-Agenten veranlasst, genehmigt und ausgeführt hat?

Maschinenidentität und Agentenverantwortung · Eintrag NGQ-033 · Version 0.3.1

> **Kürzeste Antwort** Jede Agentenhandlung sollte mit den Identitäten von Initiator, Genehmigendem und Ausführendem belegt sein.

Direkte Antwort

Erfassen Sie bei jeder folgenreichen Agentenhandlung Initiator, Genehmigenden und Ausführenden als getrennte Identitäten. Verbinden Sie sie über Handlungskennung, Ziel, genehmigten Inhalt oder Hash, Umfang, Zeitpunkt, Agenten- und Werkzeugidentitäten, Ausführungsergebnis, Beleg aus dem Zielsystem sowie Vorher- und Nachherzustand.

Einfach erklärt

Bei einer Banküberweisung können die Person, die den Auftrag erteilt, die Person, die ihn genehmigt, und das System, das das Geld bewegt, verschieden sein. Eine Zeile „Transaktion abgeschlossen“ zeigt weder, wer sie angefordert hat, noch was genehmigt wurde.

Warum ist das wichtig?

Werden die Rollen nicht getrennt, lassen sich nachträgliche Genehmigung, wiederverwendete Berechtigung, falsche menschliche Zuschreibung oder die Verwendung einer für einen anderen Gegenstand erteilten Genehmigung womöglich nicht erkennen.

Nicht verwechseln

- Initiierung: das Ereignis, das die Handlung oder den Vorschlag erzeugt.
- Genehmigung: Erlaubnis für einen bestimmten Inhalt, ein bestimmtes Ziel und einen festgelegten Umfang.
- Ausführung: technische Durchführung der Handlung.
- Zielwirkung: das Ergebnis, das im externen System tatsächlich eingetreten ist.

Was sollten Sie tun?

1. Vergeben Sie für jede Handlung eine eindeutige action_id.
2. Erfassen Sie Initiator und Nachweis der Initiierung.
3. Bewahren Sie Identität und Befugnis des Genehmigenden zusammen mit Ziel, Inhalt, Dauer und Einmalstatus der Genehmigung auf.
4. Verknüpfen Sie ausführenden Agenten, Laufzeit, Werkzeug und technische Principal-Identität.

5. Verlangen Sie eine neue Genehmigung, wenn sich Inhalt, Ziel oder Betrag nach der Genehmigung ändern.
6. Beschaffen Sie aus dem Zielsystem einen Nachweis des Ergebnisses und des Vorher-/Nachherzustands.
7. Führen Sie Wiederholungen, Teilausführung, Rücknahme und Fehler in derselben Belegkette.

Wie wird es geprüft?

- Lassen sich die Identitäten von Initiator, Genehmigendem und Ausführendem verifizieren?
- Gilt die Genehmigung genau für die ausgeführte Version?
- War die genehmigende Person oder Richtlinie für diese Handlung befugt?
- Wurde dieselbe Genehmigung erneut oder für ein anderes Ziel verwendet?
- Stimmt das Quellprotokoll mit dem Ergebnis im Zielsystem überein?
- Sind Zeitleiste und Akteurskette vollständig?
- Könnte der Datensatz nachträglich verändert worden sein?

Grenze

> Eine Trace-ID, ein Screenshot oder eine einzelne Protokollzeile ist allein kein vollständiger Beleg. Bewahren Sie genügend Kontext für die Prüfung auf und beachten Sie zugleich Datenschutz und Datenminimierung.

In einem Satz merken

> Ein belastbarer Agentendatensatz zeigt nicht nur, was geschah, sondern auch, wer es anforderte, genehmigte und ausführte.

Quellen: S23, S24, S26, S34, S35, S36, S37

Verwandte Einträge: NGQ-015, NGQ-029, NGQ-031, NGQ-032, NGQ-034

Menschliche Genehmigung, Anfechtung und Erklärung

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-034 — Wann gilt eine menschliche Genehmigung als echt, informiert, befugt und handlungsspezifisch?

Menschliche Genehmigung, Anfechtung und Erklärung · Eintrag NGQ-034 · Version 0.3.1

> **Kürzeste Antwort** Eine Genehmigung ist verlässlich, wenn die richtige Person versteht, was und warum sie genehmigt, ablehnen kann und eine bestimmte Handlung ausdrücklich erlaubt.

Direkte Antwort

Eine verlässliche menschliche Genehmigung besteht vier grundlegende Prüfungen: Die reale genehmigende Person ist verifiziert; sie besitzt für das Geschäft eine aktuelle Befugnis; wesentliche Informationen, Rolle der KI, Risiken, Alternativen und unumkehrbare Folgen werden verständlich dargestellt; und die Genehmigung ist nach Handlung, Ziel, Inhalt, Daten, Version, Betrag, Nutzungszahl und Dauer begrenzt. Das System führt anschließend nur das Genehmigte aus. Die Anwesenheit eines Menschen, der Blick auf einen Bildschirm oder ein Tastendruck sind für sich allein keine Genehmigung.

Einfach erklärt

Denken Sie an eine Überweisung. Ein allgemeines Feld „Ich genehmige Transaktionen“ genügt nicht, wenn Empfänger und Betrag fehlen. Bei einer verlässlichen Genehmigung sieht die Person Empfänger, Betrag und Folge, kann abbrechen und genehmigt nur diese Überweisung.

Warum ist das wichtig?

Eine falsche, zu breite oder uninformierte Genehmigung kann den Eindruck erwecken, ein Mensch trage die Verantwortung für eine automatisierte Entscheidung. Wendet das System das falsche Ziel, eine alte Version oder einen anderen Betrag an, bestand keine echte menschliche Kontrolle.

Nicht verwechseln

- Eine Person kann im System anwesend sein, ohne die Entscheidung geprüft zu haben.
- Eine verifizierte Person ist nicht für jedes Geschäft befugt.
- Prüfung bedeutet, Informationen zu sehen und zu bewerten; Genehmigung bedeutet, eine konkrete Handlung zu erlauben.
- Einwilligung und operative Genehmigung sind nicht derselbe rechtliche oder technische Akt.
- Eine gültige Genehmigung belegt noch nicht, dass das System genau die genehmigte Handlung ausgeführt hat.

Was sollten Sie tun?

1. Verifizieren Sie die menschliche Identität, aktuelle Rolle, Befugnis und gegebenenfalls notwendige Fachkunde des Genehmigenden.

2. Zeigen Sie Rolle der KI, wesentliche Daten, Belege, Risiken, Unsicherheit und Alternativen klar.
3. Geben Sie ausreichend Prüfzeit sowie eine echte Möglichkeit zu fragen, zu ändern, abzulehnen oder zu stoppen.
4. Binden Sie die Genehmigung an Handlung, Ziel, Inhalt, Datenumfang, Version, Betrag, Nutzungszahl und Dauer.
5. Bestätigen Sie vor einer folgenreichen oder unumkehrbaren Handlung, dass die Genehmigung weiterhin gültig ist.
6. Vergleichen Sie ausgeführte Handlung und Genehmigung Feld für Feld und verhindern Sie jede zusätzliche Handlung.
7. Bewahren Sie den Nachweis auf, wer was aufgrund welcher Information zu welchem Zeitpunkt und für welches Ergebnis genehmigte.

Wie wird es geprüft?

- Ist die Genehmigung mit einem realen Menschen und einer verifizierten Identität verbunden?
- Besaß die Person zum Geschäftszeitpunkt die erforderliche Rolle, Befugnis und Fachkunde?
- Waren wesentliche Informationen, Rolle der KI, Risiken, Unsicherheit und Alternativen sichtbar?
- Konnte die Person die Handlung tatsächlich ablehnen, ändern oder stoppen?
- War die Genehmigung an ein bestimmtes Ziel, einen Inhalt, eine Version, einen Betrag, Umfang und Zeitraum gebunden?
- War die Genehmigung abgelaufen, widerrufen oder bereits für eine andere Handlung verwendet?
- Stimmte die ausgeführte Handlung genau mit der genehmigten überein?

Grenze

> Nicht jedes Geschäft verlangt dieselbe Genehmigungsstufe. Anforderungen an wirksame Einwilligung, elektronische Signatur, Vier-Augen-Prinzip oder menschliche Aufsicht hängen von Rechtsordnung, Systemklasse, Sektor, Risiko und Auswirkung ab. Dieser Eintrag ersetzt keine Rechtsprüfung.

In einem Satz merken

> Echte Genehmigung ist nicht bloß ein Klick, sondern die informierte und befugte Erlaubnis der richtigen Person für eine konkrete Handlung.

Quellen: S24, S26, S45, S50, S62

Verwandte Einträge: NGQ-025, NGQ-026, NGQ-027, NGQ-028, NGQ-029, NGQ-030, NGQ-031, NGQ-032, NGQ-033, NGQ-035, NGQ-036, NGQ-052, NGQ-055

NGQ-035 — Wie lassen sich Genehmigungsmüdigkeit, Automationsbias und bloßes Abnicken erkennen und verhindern?

Menschliche Genehmigung, Anfechtung und Erklärung · Eintrag NGQ-035 · Version 0.3.1

> **Kürzeste Antwort** Die Qualität von Genehmigungen bemisst sich daran, ob ein Mensch Fehler findet und der KI bei Bedarf widerspricht — nicht daran, wie oft er „Ja“ sagt.

Direkte Antwort

Genehmigungsmüdigkeit entsteht, wenn viele wiederholte oder geringwertige Entscheidungen menschliche Aufmerksamkeit verbrauchen. Automationsbias entsteht, wenn eine Person einer KI-Empfehlung unangemessen hohes Gewicht gibt. Bloßes Abnicken liegt vor, wenn eine Empfehlung unter dem Anschein einer Prüfung fast automatisch angenommen wird. Zur Erkennung müssen Arbeitslast, Prüfzeit, Reihen identischer Entscheidungen, Quote erkannter KI-Fehler, begründete Änderungen und Ablehnungen, spätere Korrekturen und Ergebnisqualität gemeinsam betrachtet werden.

Einfach erklärt

Warnt Ihr Telefon jede Minute vor etwas Unwichtigem, drücken Sie irgendwann „OK“, ohne zu lesen. Dann übersehen Sie womöglich die entscheidende Warnung. Ebenso verliert menschliche Genehmigung durch unnötige Wiederholung ihre Funktion als echte Sicherheitsbarriere.

Warum ist das wichtig?

Eine erschöpfte Person oder jemand, der KI zu schnell vertraut, kann eine falsche Empfehlung genehmigen. Behandelt die Organisation eine hohe Genehmigungsquote als Compliance-Beleg, erkennt sie womöglich nicht, dass die Kontrolle wirkungslos ist.

Nicht verwechseln

- Eine hohe Genehmigungsquote belegt für sich allein keinen Automationsbias; die KI-Empfehlungen können tatsächlich richtig sein.
- Eine schnelle Entscheidung belegt für sich allein keine oberflächliche Prüfung; einfache Fälle benötigen wenig Zeit.
- Die Zahl der Übersteuerungen ist keine Qualitätskennzahl; entscheidend ist der begründete und richtige Eingriff.
- Genehmigungsmüdigkeit betrifft Arbeitslast; Automationsbias betrifft das zu hohe Gewicht einer KI-Empfehlung.
- Bloßes Abnicken bedeutet, dass ein menschlicher Name vorhanden ist, aber keine wesentliche Prüfung stattfand.

Was sollten Sie tun?

1. Verringern Sie wiederholte, risikoarme Genehmigungen und reservieren Sie menschliche Aufmerksamkeit für wesentliche, folgenreiche Entscheidungen.
2. Setzen Sie Kapazitätsgrenzen und Rotation nach Arbeitslast, Schichtdauer, Entscheidungskomplexität und Unterbrechungen ein.
3. Stellen Sie KI-Empfehlung, Belege, Unsicherheit und Gegenposition getrennt und ausgewogen dar.
4. Lassen Sie die Person bei einer Fallstichprobe zunächst unabhängig urteilen, bevor sie die KI-Empfehlung sieht.
5. Messen Sie Prüfzeit, Fehlererkennung, Änderungen, Ablehnungen, spätere Korrekturen und Ergebnisqualität gemeinsam.
6. Untersuchen Sie ungewöhnliche Muster bei Übereinstimmung, Geschwindigkeit und Fehlern nach Personengruppe und Entscheidungstyp.
7. Pausieren Sie bei sinkender Qualität den Ablauf, beheben Sie die Ursache und erneuern Sie die Schulung mit Belegen.

Wie wird es geprüft?

- Übersteigen Menge und Komplexität der Entscheidungen die tatsächliche Prüfkapazität der Person?
- Zeigen Genehmigungen ungewöhnliche Reihen mit gleicher Dauer und gleichem Ausgang?
- Können Prüfende eingebaute oder bekannte KI-Fehler erkennen?
- Sind Änderungen und Ablehnungen begründet statt zufällig?
- Werden KI-Empfehlung, Belege und Alternativen neutral dargestellt?
- Wurde die hohe Genehmigungsquote mit Ergebnisqualität und späteren Korrekturen verglichen?
- Wurden Arbeitslast und Oberflächengestaltung tatsächlich geändert, als Müdigkeits- oder Biassignale erschienen?

Grenze

> Kein einheitlicher Schwellenwert für Geschwindigkeit, Genehmigung oder Übersteuerung passt zu jeder Aufgabe. Verhaltenssignale belegen allein keine Absicht; sie sind zusammen mit Ergebnis, Risiko, Aufgabenschwierigkeit und beobachteten Fehlerdaten zu deuten.

In einem Satz merken

> Kontrolle bedeutet nicht, dass der Mensch „Ja“ sagt, sondern dass er im richtigen Moment das richtige „Nein“ sagen kann.

Quellen: S26, S38, S44, S45, S50

Verwandte Einträge: NGQ-014, NGQ-015, NGQ-026, NGQ-029, NGQ-034, NGQ-036, NGQ-038, NGQ-041, NGQ-063

NGQ-036 — Wie ist die Begründung zu erfassen, wenn ein Mensch eine KI-Empfehlung annimmt, ändert, ablehnt oder übersteuert?

Menschliche Genehmigung, Anfechtung und Erklärung · Eintrag NGQ-036 · Version 0.3.1

> **Kürzeste Antwort** Der Datensatz sollte die genaue KI-Empfehlung, die menschliche Änderung, ihren Grund und Beleg, die Befugnis der Person und das Ergebnis miteinander verbinden.

Direkte Antwort

Jede wesentliche menschliche Entscheidung wird mit einer unveränderlichen Version der tatsächlich geprüften KI-Empfehlung verknüpft. Klassifizieren Sie die Entscheidung als ACCEPT, MODIFY, REJECT oder OVERRIDE und erfassen Sie Grundcode, menschliche Erläuterung, stützende und widersprechende Belege, angewandte Regel, Befugnis und Umfang der Person, Zeitpunkt und nächsten Schritt. Eine Änderung darf die frühere Empfehlung nicht löschen. Verknüpfen Sie endgültige Entscheidung und späteres Ergebnis als getrennte Beziehungen mit dem Begründungsdatensatz.

Einfach erklärt

Stellen Sie sich eine Lehrkraft vor, die eine von KI vorgeschlagene Note ändert. Nur „Note geändert“ zu schreiben genügt nicht. Alte Note, neue Note, auslösende Antwort und angewandte Regel müssen sichtbar sein.

Warum ist das wichtig?

Ein menschlicher Eingriff ohne Begründung kann einen Fehler korrigieren oder einen neuen schaffen. Wird die frühere Empfehlung gelöscht, lässt sich nicht mehr erkennen, wer was änderte und wer für das Ergebnis verantwortlich ist.

Nicht verwechseln

- Annahme übernimmt die Empfehlung ohne wesentliche Änderung.
- Änderung korrigiert oder begrenzt einen Teil der Empfehlung durch menschliche Entscheidung.
- Ablehnung bedeutet, dass die Empfehlung nicht angewendet wird.
- Übersteuerung bedeutet, dass eine befugte menschliche Entscheidung eine frühere Entscheidung oder ein automatisiertes Ergebnis verdrängt.
- Ein Grundcode unterstützt die Klassifizierung; Freitext liefert den konkreten Kontext.

Was sollten Sie tun?

1. Fixieren Sie die geprüfte KI-Empfehlung mit Identität, Modell, Version, Prompt, Daten und Zeitpunkt.

2. Klassifizieren Sie die menschliche Entscheidung ausdrücklich als ACCEPT, MODIFY, REJECT oder OVERRIDE.
3. Erfassen Sie Grundcode und kurze, konkrete menschliche Erläuterung.
4. Verknüpfen Sie stützende Belege, Gegenbelege, angewandte Regel und Unsicherheit mit der Entscheidung.
5. Bewahren Sie Identität, Rolle, Befugnis und einschlägigen Interessen- oder Konfliktstatus des Entscheidenden.
6. Verbinden Sie geänderte Felder, endgültige Entscheidung und ausgeführte Handlung, ohne die frühere Empfehlung zu löschen.
7. Fügen Sie das spätere Ergebnis und jede erneute Prüfung derselben Entscheidungskette hinzu.

Wie wird es geprüft?

- Kann die genaue KI-Empfehlung samt Version später geprüft werden?
- Wurde der Typ der menschlichen Entscheidung richtig und einheitlich klassifiziert?
- Erklärt die Begründung die konkrete Änderung oder enthält sie nur ein allgemeines Etikett?
- Sind stützende und widersprechende Belege gemeinsam sichtbar?
- Sind Rolle, Befugnis und möglicher Interessenkonflikt des Entscheidenden erfasst?
- Wurden frühere Empfehlung oder ungünstige Belege gelöscht?
- Stimmen begründete Entscheidung, ausgeführte Handlung und tatsächliches Ergebnis überein?

Grenze

> Ein Begründungsdatensatz muss nicht jeden inneren Gedanken oder geschützte Tatsache offenlegen. Datenschutz, Sicherheit und rechtliche Vertraulichkeit können Details begrenzen; der für Prüfung und wirksame Anfechtung wesentliche Grund darf jedoch nicht vollständig unsichtbar werden.

In einem Satz merken

> Wurde die Entscheidung geändert, muss nachvollziehbar sein, was, warum und unter wessen Befugnis geändert wurde.

Quellen: S26, S35, S36, S37, S44, S50

Verwandte Einträge: NGQ-026, NGQ-029, NGQ-032, NGQ-033, NGQ-034, NGQ-035, NGQ-037, NGQ-039, NGQ-040, NGQ-044

NGQ-037 — Wie sollten Anfechtung, erneute Prüfung, Korrektur und Rechtsbehelf bei einer KI-gestützten Entscheidung funktionieren?

Menschliche Genehmigung, Anfechtung und Erklärung · Eintrag NGQ-037 · Version 0.3.1

> **Kürzeste Antwort** Die betroffene Person sollte die Entscheidung verstehen, falsche Daten korrigieren, neue Belege vorlegen und eine befugte menschliche Prüfung erreichen können.

Direkte Antwort

Ein wirksamer Mechanismus teilt Entscheidung und Auswirkung zugänglich mit, erklärt Rolle der KI und wesentliche Gründe, nimmt Berichtigungen von Identität, Daten und Belegen entgegen, bietet bei drohendem schwerem Schaden vorläufigen Schutz und ermöglicht die Prüfung durch eine befugte, hinreichend unabhängige Person, die die erste Entscheidung tatsächlich ändern kann. Das begründete Ergebnis wird mitgeteilt. Eine Korrektur bleibt nicht in einer Datei: Sie wird an die betroffene Entscheidung, Datenbestände und verbundenen Folgesysteme verteilt.

Einfach erklärt

Ist Ihre Rechnung falsch, ist dieselbe automatische Berechnung noch einmal auszuführen keine Prüfung. Sie müssen den falschen Posten benennen, Ihren Nachweis einreichen und eine Person erreichen, die die Rechnung wirklich ändern kann.

Warum ist das wichtig?

Eine falsche Identität, Datenangabe oder Modellausgabe kann Beschäftigung, Leistungen, Zahlungen und Ruf real schädigen. Ist der Weg unklar oder wirkungslos, bleibt die Person im selben fehlerhaften System gefangen.

Nicht verwechseln

- Korrektur richtet sich auf die Berichtigung unzutreffender Daten oder Datensätze.
- Erneute Prüfung untersucht dieselbe Entscheidung mit neuen oder neu bewerteten Belegen.
- Eine Anfechtung erlaubt der betroffenen Person, Gründe gegen Entscheidung oder Verfahren vorzubringen.
- Ein Rechtsbehelf ist, soweit vorgesehen, die Prüfung durch eine höhere oder andere befugte Stelle.
- Abhilfe behandelt neben dem Stoppen des Fehlers auch den entstandenen Schaden.

Was sollten Sie tun?

1. Teilen Sie Entscheidung, Wirkung, Rollen von KI und Mensch, Hauptgrund, Frist und Anfechtungsweg zugänglich mit.

2. Bieten Sie einen sicheren Kanal für Identitäts- und Datenkorrektur, neue Belege und Verfahrenseinwände.
3. Registrieren Sie den Fall unter einer Kennung und zeigen Sie Verantwortlichen, Status, Frist und nächsten Schritt.
4. Prüfen Sie bei möglichem schwerem oder unumkehrbarem Schaden eine vorläufige Aussetzung oder Schutzmaßnahme.
5. Gewährleisten Sie eine befugte, kompetente und hinreichend unabhängige menschliche Prüfung, die die erste Entscheidung ändern kann.
6. Teilen Sie Ergebnis, verwendete Belege, Gründe für Annahme oder Ablehnung und verbleibende Rechtsbehelfe mit.
7. Verteilen Sie die Korrektur an jedes betroffene System und testen Sie das Live-Ergebnis.

Wie wird es geprüft?

- Kann die betroffene Person Entscheidung, Wirkung und Anfechtungsweg verstehen?
- Ist der Kanal zugänglich, sicher und praktisch nutzbar?
- Werden neue Belege und Datenkorrekturen inhaltlich geprüft?
- Wurde dieselbe KI mit denselben Daten erneut ausgeführt und als unabhängige Prüfung dargestellt?
- Kann der menschliche Prüfer eine andere Entscheidung treffen und durchsetzen?
- Wurden bei einem Hochrisikofall vorläufiger Schutz und Friststeuerung berücksichtigt?
- Wurde eine angenommene Korrektur in verbundenen Systemen und im Live-Ergebnis verifiziert?

Grenze

> Nicht jede Entscheidung gewährt dasselbe formelle Recht auf Anfechtung oder Rechtsbehelf. Fristen, zuständige Stellen, Offenlegung und Abhilfe richten sich nach Rechtsordnung, Sektor, Vertrag und Auswirkung; eine qualifizierte Fachperson sollte das anwendbare Verfahren bestimmen.

In einem Satz merken

> Anfechtung bedeutet nicht, derselben Maschine dieselbe Frage noch einmal zu stellen.

Quellen: S45, S48, S50, S61, S62

Verwandte Einträge: NGQ-014, NGQ-015, NGQ-026, NGQ-034, NGQ-036, NGQ-038, NGQ-039, NGQ-045, NGQ-051, NGQ-064

NGQ-038 — Wann gilt eine Person, ein Gremium oder eine Einheit, die eine KI-gestützte Entscheidung prüft, als unabhängig und unparteiisch?

Menschliche Genehmigung, Anfechtung und Erklärung · Eintrag NGQ-038 · Version 0.3.1

> **Kürzeste Antwort** Die prüfende Stelle muss von erster Entscheidung und Interessenkonflikten hinreichend getrennt sein, die vollständigen Unterlagen sehen und ein anderes Ergebnis durchsetzen können.

Direkte Antwort

Unabhängigkeit entsteht nicht allein durch den Namen einer anderen Person, Abteilung oder Organisation. Prüfende oder Gremium sind funktional von den Urhebern der ersten Entscheidung und den an einem bestimmten Ausgang Interessierten getrennt, legen wesentliche und persönliche Interessen offen, sind vor unzulässigen Weisungen geschützt, haben Zugang zu vollständigen und ausgewogenen Belegen, besitzen notwendige Fachkunde und können die Entscheidung bestätigen, ändern, zurücknehmen oder berichtigen. Unparteilichkeit verlangt, günstige und ungünstige Belege nach derselben Methode zu bewerten.

Einfach erklärt

Es ist problematisch, wenn ein Schiedsrichter für eine der Mannschaften arbeitet. Ein anderes Trikot genügt nicht: Er darf keine Anweisungen von einem Team erhalten, muss die Regeln kennen und eine Entscheidung treffen können, die tatsächlich umgesetzt wird.

Warum ist das wichtig?

Eine scheinbar getrennte, praktisch aber vom ursprünglichen Entscheider kontrollierte Prüfung setzt nur eine zweite Unterschrift unter denselben Fehler. Bleiben Interessen und Befugnisse verborgen, gibt es keinen echten Korrekturweg.

Nicht verwechseln

- Unabhängigkeit bedeutet hinreichende Trennung von Entscheidungs- und Druckkette.
- Unparteilichkeit bedeutet, Belege nicht auf ein vorgegebenes Ergebnis hin zu verbiegen.
- Fachkunde ist das Wissen und Können, das zur Beurteilung der Sache nötig ist.
- Auch eine andere Person kann abhängig sein, wenn derselbe Vorgesetzte Druck für ein bestimmtes Ergebnis ausübt.
- Ein anderes KI-Modell ist für sich allein keine menschliche oder unabhängige erneute Prüfung.

Was sollten Sie tun?

1. Trennen Sie ursprünglichen Entscheider, interessierte Partei, Prüfer und letzte Instanz in einer Rollenmatrix.
2. Verlangen Sie die schriftliche Offenlegung finanzieller, persönlicher, organisatorischer, fachlicher und leistungsbezogener Konflikte.
3. Ist ein Konflikt nicht beherrschbar, nutzen Sie Ausschluss, Ersatzprüfer oder ein ausgewogenes Gremium.
4. Geben Sie vollständige Akte, Gegenbelege, Entscheidungspfad und Zugang zu notwendiger technischer Expertise.
5. Legen Sie Prüfumfang, Maßstab und mögliche Ergebnisse im Voraus fest.
6. Verifizieren Sie im realen Verfahren, dass eine andere Entscheidung getroffen und durchgesetzt werden kann.
7. Bewahren Sie Druckversuche, Belegbeschränkungen, abweichende Meinungen und Ausschlussentscheidungen im Prüfpfad.

Wie wird es geprüft?

- Hat der Prüfer die erste Entscheidung vorbereitet oder profitiert er unmittelbar vom Ergebnis?
- Erzeugen Berichtslinien oder Leistungsziele unzulässigen Ergebnisdruck?
- Wurden Interessenkonflikte vollständig offengelegt und behandelt?
- Kann der Prüfer auf alle wesentlichen Belege für und gegen die Entscheidung zugreifen?
- Ist die notwendige rechtliche, technische oder fachliche Kompetenz vorhanden?
- Kann der Prüfer die erste Entscheidung wirklich ändern und die Änderung umsetzen lassen?
- Wurde ein anderer Name von Person, Abteilung oder Modell als ausreichender Unabhängigkeitsnachweis behandelt?

Grenze

> Vollständige organisatorische Trennung ist nicht immer möglich. Unabhängigkeit ist eine Frage von Grad und Kontext; Grenzen sind offenzulegen, und mit steigendem Risiko sind stärkere Funktionstrennung oder externe Prüfung einzusetzen. Dieser Eintrag verleiht keine Prüferakkreditierung.

In einem Satz merken

> Ein anderer Name ist keine Unabhängigkeit; unabhängig ist eine geschützte Stellung, aus der eine andere Entscheidung getroffen werden kann.

Quellen: S26, S44, S45, S50, S61

Verwandte Einträge: NGQ-026, NGQ-029, NGQ-034, NGQ-035, NGQ-036, NGQ-037, NGQ-039, NGQ-063

NGQ-039 — Welche Informationen muss die Erklärung einer KI-gestützten Entscheidung enthalten, damit die betroffene Person sie wirksam anfechten kann?

Menschliche Genehmigung, Anfechtung und Erklärung · Eintrag NGQ-039 · Version 0.3.1

> **Kürzeste Antwort** Die Erklärung sollte nicht nur zeigen, was dieser Person geschah, sondern auch, welche Daten, Regeln sowie KI- und Menschenrollen das Ergebnis wesentlich beeinflussten.

Direkte Antwort

Eine wirksame Erklärung nennt zuerst die genaue Entscheidung und ihre Wirkung auf die Person. Danach zeigt sie Rollen von KI und Menschen, wesentliche verwendete Daten samt Quelle sowie Regeln, Schwellenwerte und Unsicherheiten, die das Ergebnis beeinflussten. Fehlende oder korrigierbare Angaben und der Anfechtungsweg müssen ebenfalls klar sein. „Der Algorithmus hat es berechnet“ erklärt nicht, warum dieses Ergebnis entstand.

Einfach erklärt

Wird ein Antrag abgelehnt, hilft „Das System hat Sie als nicht berechtigt eingestuft“ nicht. Sie müssen wissen, welche Angabe als falsch oder fehlend galt, welche Regel angewandt wurde und was Sie berichtigen oder bestreiten können.

Warum ist das wichtig?

Ohne wesentlichen Grund kann eine Person weder falsche Daten korrigieren noch Gegenbelege einreichen oder die Entscheidung sinnvoll anfechten. Eine geschliffene, aber sachfremde Darstellung erzeugt nur den Anschein von Transparenz.

Nicht verwechseln

- Eine allgemeine Systemerklärung beschreibt das Modell grob; eine entscheidungsspezifische Erklärung beschreibt das konkrete Ergebnis.
- Eine Datenerklärung benennt verwendete Informationen; eine Faktorenerklärung zeigt deren Einfluss auf das Ergebnis.
- Eine Erklärung nennt Entscheidungsgründe; sie macht die Entscheidung nicht automatisch richtig oder rechtmäßig.
- Offenlegung stellt Informationen bereit; eine wirksame Anfechtungserklärung muss ausreichend handlungsorientiert sein.
- Vertrauliche oder sicherheitsrelevante Angaben können geschützt sein, doch der wesentliche Grund darf nicht vollständig verborgen werden.

Was sollten Sie tun?

1. Nennen Sie Entscheidungskennung, Datum, Umfang, Wirkung und Fortgeltung.
2. Trennen Sie Rollen von KI-System, menschlichem Prüfer und letztem Entscheider.
3. Benennen Sie wesentliche Daten, Quelle, Datum und Zuordnung zur Person.
4. Erklären Sie Faktoren, Regeln, Schwellenwerte und wesentliche Gegenbelege, die dieses Ergebnis beeinflussten.
5. Machen Sie Unsicherheit, fehlende Angaben und Grenzen der Erklärung sichtbar.
6. Nennen Sie korrigierbare Daten, einreichbare neue Belege, Frist und sicheren Anfechtungsweg.
7. Prüfen Sie die Erklärung am tatsächlichen Entscheidungsdatensatz und auf Verständlichkeit für die Zielperson.

Wie wird es geprüft?

- Kann die Person verstehen, welche Entscheidung und Wirkung sie betrifft?
- Sind die Grenzen zwischen KI- und Menschenrollen richtig beschrieben?
- Sind wesentliche Daten, Quelle, Datum und Entitätszuordnung sichtbar?
- Werden die Faktoren und Regeln erklärt, die das Ergebnis tatsächlich beeinflussten?
- Wurde eine allgemeine Modellbeschreibung als entscheidungsspezifische Erklärung ausgegeben?
- Weiß die Person, was sie wo korrigieren oder anfechten kann?
- Wurden Datenschutz oder Geschäftsgeheimnisse vorgeschoben, um den wesentlichen Grund vollständig zu verbergen?

Grenze

> Der erforderliche Umfang einer Erklärung hängt von Rechtsordnung, Entscheidungsart und Risiko ab. Sicherheit, Rechte Dritter und rechtliche Vertraulichkeit können Details begrenzen. Das Vorhandensein einer Erklärung belegt für sich allein weder Richtigkeit noch Fairness oder Rechtmäßigkeit.

In einem Satz merken

> Eine Erklärung, die keine Anfechtung ermöglicht, ist nur der Anschein von Information.

Quellen: S35, S45, S48, S50, S61, S62

Verwandte Einträge: NGQ-007, NGQ-014, NGQ-021, NGQ-026, NGQ-036, NGQ-037, NGQ-038, NGQ-040, NGQ-043

NGQ-040 — Wie weist eine Organisation nach, dass eine KI-Erklärung den wirklichen Entscheidungsprozess getreu wiedergibt und nicht nachträglich erfunden wurde?

Menschliche Genehmigung, Anfechtung und Erklärung · Eintrag NGQ-040 · Version 0.3.1

> **Kürzeste Antwort** Eine plausible Darstellung genügt nicht; die Erklärung muss durch versionierte Datensätze vom Entscheidungszeitpunkt und durch Verhaltenstests gestützt sein.

Direkte Antwort

Verknüpfen Sie die Erklärung mit einem Datensatz, der bei der Entscheidung bewahrt wurde. Er zeigt Modell- und Systemversionen, Prompts, verwendete Daten, ausgewählte Informationen, Richtlinie, Werkzeugaufrufe, menschliche Eingriffe und angewandtes Ergebnis. Ordnen Sie jede wesentliche Aussage der Erklärung einem dieser Belege zu. Entfernen oder verändern Sie, soweit angemessen, einen behaupteten Faktor und prüfen Sie, ob sich das Ergebnis ändert. Stützt der Datensatz den Text nicht, kennzeichnen Sie ihn als mögliche nachträgliche Darstellung statt als getreue Erklärung.

Einfach erklärt

Stellen Sie sich eine Restaurantrechnung vor, die nach dem Essen aus dem Gedächtnis geschrieben wird. Der Gesamtbetrag kann richtig aussehen, belegt aber nicht, welche Speisen bestellt wurden. Eine verlässliche Rechnung stimmt mit den bei der Bestellung entstandenen Aufzeichnungen überein.

Warum ist das wichtig?

Menschen vertrauen leicht einer vernünftig klingenden Erklärung. Ist sie nicht an die reale Entscheidung gebunden, sollen sie womöglich die falschen Daten korrigieren, der eigentliche Fehler bleibt verborgen oder Verantwortung wird falsch zugeordnet.

Nicht verwechseln

- Eine plausible Erklärung klingt verständlich; eine getreue Erklärung stimmt mit den Belegen der realen Entscheidung überein.
- Eine nachträgliche Erklärung entsteht nach der Entscheidung und kann richtig oder erfunden sein.
- Provenienz fragt, woher ein Datensatz stammt; Kausalität fragt, welches Element das Ergebnis veränderte.
- Ein Ereignisprotokoll beweist nicht, dass es vollständig, richtig oder unverändert ist.
- Reproduktion sucht ein ähnliches Ergebnis; ein Treuetest untersucht die Kausalaussage der Erklärung.

Was sollten Sie tun?

1. Bewahren Sie zeitpunktbezogene Kopien von Modell, Daten, Prompt, Richtlinie, Werkzeugen und menschlichen Versionen.
2. Erstellen Sie eine zeitlich verknüpfte Spur von Eingaben, Informationsauswahl, Werkzeugaufrufen, menschlichen Eingriffen und angewandtem Ergebnis.
3. Schützen Sie Ereignisdatensatz und Entscheidungsabbild mit Hashes, Zugriffskontrollen und Änderungspfad.
4. Ordnen Sie jede wesentliche Aussage der Erklärung dem stützenden Entscheidungsdatensatz zu.
5. Prüfen Sie, soweit angemessen, Verhaltenstreue durch Faktorentfernung, Gegenfaktum, Wiederholung und Sensitivitätstests.
6. Geben Sie unbelegte oder nur mögliche Darstellungen nicht als getreue Erklärung aus; nennen Sie das Sicherheitsniveau.
7. Validieren Sie die Erklärung bei einer Systemänderung erneut, statt sie unverändert auf die neue Version zu übertragen.

Wie wird es geprüft?

- Ist die Erklärung mit der richtigen Entscheidungskennung und einem Abbild vom Entscheidungszeitpunkt verbunden?
- Lassen sich Modell, Prompt, Daten, Informationsauswahl, Werkzeuge, Richtlinie und menschliche Eingriffe verfolgen?
- Erscheint jeder wesentliche Grund der Erklärung tatsächlich im Datensatz?
- Sind Vollständigkeit und Integrität der Ereignisdatensätze geschützt?
- Wurde Verhaltenstreue getestet oder nur die sprachliche Qualität bewertet?
- Wurde eine nachträgliche oder anbietergenerierte Erklärung als sichere interne Ursache dargestellt?
- Wurde nach einem Versionswechsel eine alte Erklärung ohne erneute Validierung verwendet?

Grenze

> Bei undurchsichtigen und komplexen Modellen lässt sich vollständige interne Kausalität nicht immer belegen. Eine Entscheidungsspur zeigt nur den beobachtbaren Prozess und legt womöglich nicht jeden internen Mechanismus offen. Dann sind Sicherheitsniveau und Unbekanntes ausdrücklich zu nennen.

In einem Satz merken

> Eine gute Geschichte kann eine Erklärung sein; Treue verlangt Belege vom Moment der Entscheidung.

Quellen: S26, S35, S36, S37, S44, S50

Verwandte Einträge: NGQ-014, NGQ-021, NGQ-029, NGQ-033, NGQ-036, NGQ-039, NGQ-041, NGQ-044, NGQ-063

Entscheidungslebenszyklus, Korrektur und Vergessen

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-041 — Was bedeutet es, wenn sich eine KI-gestützte Entscheidung aus denselben Eingaben nicht reproduzieren lässt, und wie sollte Reproduzierbarkeit geprüft werden?

> **Kürzeste Antwort** Ein anderes Ergebnis belegt keinen Angriff; probabilistische Streuung, ein unvollständiges Entscheidungspaket, Versionsdrift, Fehler und Manipulation müssen getrennt geprüft werden.

Direkte Antwort

„Dieselbe Eingabe“ ist nicht nur derselbe Satz des Nutzers. Zum Entscheidungspaket gehören Modell- und Systemversion, Prompts, Informationsauswahl, zeitbezogene Datenkopie, Werkzeugergebnisse, Richtlinie, menschlicher Eingriff, Zeitpunkt, Land, Sprache, Konfiguration und, soweit möglich, Zufallszustand. Bestimmen Sie zuerst die verlangte Gleichwertigkeit: wortgleiche Formulierung, dieselben wesentlichen Aussagen, dieselbe Klasse oder dieselbe Handlung. Messen Sie Streuung durch Wiederholungs- und Bedingungsvergleiche. Überschreitet die Abweichung den erwarteten Bereich, beginnen Sie eine Ursachenanalyse.

Einfach erklärt

Dasselbe Rezept zweimal zu kochen garantiert nicht, dass jeder Bissen gleich aussieht. Enthält ein Gericht jedoch Salz und das andere Zucker, lässt sich das nicht mit der Variabilität des Kochens abtun. Zutaten, Ofen, Zeit und Rezeptversion müssen geprüft werden.

Warum ist das wichtig?

Wer erwartbare Streuung als Fehler behandelt, erzeugt unnötige Alarme; wer echte Versions- oder Datendrift als Zufall abtut, verdeckt schwerwiegende Entscheidungsunterschiede. Ein unvollständiges Entscheidungspaket schwächt zudem Erklärung und Anfechtung.

Nicht verwechseln

- Derselbe Text bedeutet nicht dieselbe Informationsauswahl, dasselbe Werkzeugergebnis oder denselben Zeitkontext.
- Exakte Ausgabegleichheit verlangt Wort-für-Wort-Übereinstimmung.
- Semantische Gleichwertigkeit akzeptiert unterschiedliche Formulierungen mit derselben wesentlichen Bedeutung.
- Entscheidungsgleichwertigkeit fragt, ob trotz unterschiedlicher Ausgabe dieselbe befugte Handlung folgt.

- Wiederholbarkeit betrifft dasselbe Team und dieselben Bedingungen; Reproduzierbarkeit erlaubt auch ein hinreichend ausgestattetes anderes Team oder Umfeld.

Was sollten Sie tun?

1. Definieren Sie Reproduktionsobjekt und zulässige Gleichwertigkeitsstufe im Voraus.
2. Bewahren Sie das Entscheidungspaket: Modell, Daten, Prompt, Informationsauswahl, Werkzeuge, Richtlinie, Personen, Zeit und Umgebung.
3. Führen Sie unter gleichen Bedingungen genügend Wiederholungen aus, um normale Ausgabeverteilung und Entscheidungswechsel zu messen.
4. Ändern Sie Version, Sprache, Land und Zeit einzeln, um die ergebniswirksame Bedingung zu erkennen.
5. Klassifizieren Sie die Abweichung als erwartbare Streuung, fehlende Eingabe, Versions- oder Datendrift, Implementierungsfehler, externen Zustand oder Manipulation.
6. Lösen Sie menschliche Prüfung und Vorfallverfahren aus, wenn sich eine kritische Entscheidungsklasse ändert.
7. Ermöglichen Sie einem hinreichend unabhängigen Team, das Ergebnis aus dem aufgezeichneten Paket zu testen und die Grenzen zu berichten.

Wie wird es geprüft?

- Ist das Reproduktionsziel auf Ebene von Wortlaut, Bedeutung, Entscheidung oder Handlung klar?
- Wurden alle wesentlichen Bestandteile des realen Entscheidungspakets bewahrt?
- Wurde Erfolg oder Scheitern aus einer einzigen Wiederholung abgeleitet?
- Wurden Drift von Modell, Daten, Informationsauswahl, Werkzeugen, Richtlinie und Zeit untersucht?
- Wurden kritische Entscheidungswechsel in einem mittleren Ähnlichkeitswert verborgen?
- Kann eine unabhängige Reproduktion auf dieselben Belege und Entscheidungsregeln zugreifen?
- Blieben ungeklärte Unterschiede UNRESOLVED, statt mit Scheingewissheit erklärt zu werden?

Grenze

> In geschlossenen Drittsystemen lassen sich Modellzustand, Serverkonfiguration oder Zufall womöglich nicht vollständig bewahren. Selbst mit demselben Entscheidungspaket können probabilistische Unterschiede auftreten. Fehlende Reproduktion belegt für sich allein weder Fehler oder Angriff noch eine falsche Entscheidung.

In einem Satz merken

> Derselbe Satz ist nicht dasselbe Entscheidungspaket.

Quellen: S35, S36, S37, S38, S50, S51, S52

Verwandte Einträge: NGQ-012, NGQ-014, NGQ-029, NGQ-033, NGQ-035, NGQ-040, NGQ-042, NGQ-060, NGQ-062, NGQ-063

NGQ-042 — Sollten frühere Entscheidungen neu bewertet werden, wenn sich Modell, Daten, Prompt, Richtlinie oder Werkzeugversion eines KI-Systems ändern?

Entscheidungslebenszyklus, Korrektur und Vergessen · Eintrag NGQ-042 · Version 0.3.1

> **Kürzeste Antwort** Nicht jede Änderung öffnet jede frühere Entscheidung neu; eine risikobasierte Neubewertung ist nötig, wenn Richtigkeit oder fortwirkende Folgen wesentlich betroffen sein könnten.

Direkte Antwort

Erfassen Sie zuerst Version, Zweck, Umfang und wesentliche Wirkung der Änderung. Ermitteln Sie dann, welche früheren Entscheidungsklassen sich hinsichtlich Identität, Daten, Belegen, Befugnis, Erklärung, Sicherheit, Fairness, Rechtswirkung oder verbundenen Folgehandlungen ändern könnten. Messen Sie Auswirkungen, soweit möglich, durch Stichproben und Vergleichstests. Prüfen Sie kritische oder fortwirkende Ergebnisse gezielt neu. Eine neue Version korrigiert eine frühere Entscheidung nicht automatisch, und eine neue Regel macht sie nicht automatisch falsch.

Einfach erklärt

Wird die Software einer Waage repariert, müssen Sie vielleicht nicht jeden Karton des Vorjahres erneut wiegen. Stellt sich aber heraus, dass die alte Waage in einem bestimmten Bereich systematisch zu wenig anzeigte, prüfen Sie wichtige, darauf beruhende Entscheidungen erneut.

Warum ist das wichtig?

Jede frühere Entscheidung blind zu wiederholen verursacht unverhältnismäßige Kosten; nichts neu zu öffnen lässt bekannte Fehler Menschen und Systeme weiter beeinträchtigen.

Nicht verwechseln

- Ein Versionswechsel ist ein technisches Ereignis; seine wesentliche Wirkung benötigt eigene Belege.
- Eine heutige Korrektur ändert eine frühere Entscheidung nicht von selbst.
- Historische Richtigkeit wird nach Informationen und Regeln der damaligen Zeit beurteilt; aktuelle Gültigkeit nach dem heutigen Zustand.
- Rückwirkende Wirkungsanalyse bestimmt die Risikogruppe; Neufeststellung entscheidet den Einzelfall erneut.
- Fortwirkende Wirkung bedeutet, dass eine frühere Entscheidung heute noch Folgen für eine Person oder ein System erzeugt.

Was sollten Sie tun?

1. Vergleichen Sie geändertes Modell, Daten, Prompt, Richtlinie, Werkzeug und Konfiguration Feld für Feld mit der Vorversion.
2. Erfassen Sie Zweck, Grund, Verantwortlichen, Datum und erwartete Entscheidungswirkung in einem Änderungspaket.
3. Bestimmen Sie betroffene Entscheidungstypen, Zeiträume, Personengruppen, Entitäten und verbundene Folgeergebnisse.
4. Vergleichen Sie alte und neue Version unter denselben Bedingungen an repräsentativen Fällen.
5. Eröffnen Sie bei kritischem Fehler, falscher Person, fortdauerndem Schaden oder rechtlichem Auslöser eine gezielte Prüfung.
6. Berichtigen Sie neu bewertete Entscheidungen und verteilen Sie das Ergebnis an jedes betroffene System.
7. Dokumentieren Sie mit Gründen den als unbetroffen angenommenen Umfang, Ausnahmen und verbleibende Unsicherheit.

Wie wird es geprüft?

- Sind alle geänderten Bestandteile und Versionen erfasst?
- Wurde die Änderung ohne Wirkungstest als unwesentlich behandelt?
- Wurden betroffene Daten, Entscheidungen, Personen und Folgesysteme bestimmt?
- Wurden alte und neue Version unter denselben Bedingungen verglichen?
- Wurden kritische Entscheidungen mit fortwirkenden Folgen neu bewertet?
- Hat die neue Version historische Datensätze still überschrieben?
- Gibt es Belege für das berichtigte Live-Ergebnis und seine Verteilung?

Grenze

> Rückwirkende Prüfung und Rechtswirkung einer früheren Entscheidung hängen von Bestandskraft, Rechten, Verträgen, Sektor und Rechtsordnung ab. Eine technische Änderung allein bedeutet weder, dass jede Entscheidung neu eröffnet werden muss, noch dass sie unwirksam ist.

In einem Satz merken

> Das System zu aktualisieren berichtigt die Vergangenheit nicht automatisch.

Quellen: S35, S38, S41, S44, S45, S50

Verwandte Einträge: NGQ-014, NGQ-021, NGQ-029, NGQ-040, NGQ-041, NGQ-043, NGQ-044, NGQ-045, NGQ-064, NGQ-067

NGQ-043 — Wie ist die historische Richtigkeit einer früheren KI-gestützten Entscheidung von ihrer heutigen Fortgeltung zu unterscheiden?

Entscheidungslebenszyklus, Korrektur und Vergessen · Eintrag NGQ-043 · Version 0.3.1

> **Kürzeste Antwort** Eine Entscheidung kann bei Erlass richtig gewesen sein und heute wegen Ablauf, Rücknahme oder geänderter Bedingungen nicht mehr gelten.

Direkte Antwort

Bewerten Sie jede Entscheidung anhand mindestens zweier Zeitfragen. Historische Richtigkeit fragt, ob das Ergebnis zum Entscheidungszeitpunkt durch Tatsachen, Quellen, Regeln und Befugnis gestützt war. Aktuelle Gültigkeit fragt, ob die Entscheidung heute noch aktiv und weder abgelaufen, ausgesetzt, zurückgenommen, berichtigt noch ersetzt ist. Eine frühere Entscheidung kann auch nach Verlust ihrer Gültigkeit weiter Folgen erzeugen; diese Folgen sind gesondert zu erkennen und zu beheben.

Einfach erklärt

Ein Führerschein, der im Vorjahr gültig war, war damals echt. Ist er heute abgelaufen, wird das alte Dokument dadurch nicht falsch; es berechtigt nur nicht mehr zum heutigen Fahren.

Warum ist das wichtig?

Gehen Zeitangaben verloren, kann eine alte Entscheidung als aktuelle Befugnis verwendet oder eine heutige Änderung fälschlich auf die Vergangenheit übertragen werden. Bleiben fortwirkende Folgen unsichtbar, kann eine abgelaufene Entscheidung die Person weiter beeinträchtigen.

Nicht verwechseln

- Historische Richtigkeit ist Übereinstimmung mit den Tatsachen zum Bezugszeitpunkt der Entscheidung.
- Historische Gültigkeit fragt, ob die Entscheidung damals befugt und wirksam war.
- Aktuelle Richtigkeit fragt, ob die zugrunde liegenden Tatsachen heute noch stimmen.
- Aktuelle Gültigkeit fragt, ob die Entscheidung heute noch rechtliche oder operative Wirkung trägt.
- Fortwirkende Wirkung bedeutet, dass eine nicht mehr gültige Entscheidung in Systemen weiterhin Folgen erzeugt.

Was sollten Sie tun?

1. Speichern Sie Entscheidungszeit, Bezugszeit, Wirksamkeitsbeginn und Gültigkeitsende in getrennten Feldern.
2. Bewahren Sie die zum Entscheidungszeitpunkt gültigen Versionen von Daten, Regeln, Modell, menschlicher Befugnis und Belegen.

3. Erfassen Sie aktiv, ausgesetzt, abgelaufen, zurückgenommen, berichtigt und ersetzt als getrennte Zustände.
4. Halten Sie bei einer aktuellen Abfrage sowohl den Gegenwartszustand als auch seine Ereigniskette zugänglich.
5. Suchen Sie nach fortwirkenden Folgen bei Profilen, Zahlungen, Zugang, Empfehlungen und Repräsentation.
6. Verknüpfen Sie neue und alte Entscheidung mit ausdrücklicher Beziehung und Wirksamkeitsdatum.
7. Verifizieren Sie die Korrektur auf betroffenen Live- und Folgeoberflächen.

Wie wird es geprüft?

- Sind Entscheidungszeit und Bezugszeit von Daten und Regel getrennt?
- Sind Beginn und Ende der Gültigkeit erfasst?
- Wird eine frühere Entscheidung als aktuelle Befugnis statt als historischer Datensatz verwendet?
- Hat neue Information die Beurteilung der damaligen Richtigkeit unzulässig verändert?
- Sind Beziehungen zu Aussetzung, Rücknahme, Korrektur und Ersetzung sichtbar?
- Wurde nach fortwirkenden Folgen einer ungültigen Entscheidung gesucht?
- Wählt das Live-System die aktuelle befugte Entscheidung aus?

Grenze

> Historische Richtigkeit und rechtliche Gültigkeit sind nicht dasselbe; die Wirkung einer früheren Entscheidung kann vom anwendbaren Recht bestimmt werden. Eine heute falsch wirkende Tatsache beweist nicht, dass sie schon beim Erlass falsch war.

In einem Satz merken

> Eine gestern richtige Entscheidung gilt heute nicht zwangsläufig weiter.

Quellen: S14, S15, S35, S44, S50

Verwandte Einträge: NGQ-014, NGQ-021, NGQ-036, NGQ-039, NGQ-042, NGQ-044, NGQ-045, NGQ-046

NGQ-044 — Wie sind Wirksamkeitsbeginn, Ende, Aussetzung, Rücknahme, Korrektur und ersetzende Entscheidung einer KI-gestützten Entscheidung maschinenlesbar zu erfassen?

Entscheidungslebenszyklus, Korrektur und Vergessen · Eintrag NGQ-044 · Version 0.3.1

> **Kürzeste Antwort** Lassen Sie die Entscheidung unverändert und fügen Sie jede Lebenszyklusänderung als eigenes Ereignis mit Kennung, Zeit, befugtem Akteur, Grund und Verbindung zwischen vorherigem und folgendem Zustand hinzu.

Direkte Antwort

Jede Entscheidung erhält eine dauerhafte Entscheidungskennung und eine unveränderliche Version. Erstellung, Inkrafttreten, Aussetzung, Rücknahme, Korrektur, Ablauf und Ersetzung werden als zusätzliche Ereignisse gespeichert, ohne den früheren Datensatz zu löschen. Jedes Ereignis enthält Ereigniskennung, Zeit, Akteur, Befugnis, Grund, früheren Zustand, neuen Zustand, Beleg und Zielversion. Der aktuelle Zustand wird aus diesen befugten Ereignissen abgeleitet; er ersetzt die Ereignishistorie nicht.

Einfach erklärt

Denken Sie an einen Kontoauszug. Der heutige Saldo erscheint als eine Zahl, doch Ein- und Ausgänge bleiben erhalten, damit seine Entstehung nachvollziehbar ist. Ebenso wird der aktuelle Zustand einer Entscheidung aus ihrer Ereignishistorie berechnet.

Warum ist das wichtig?

Das Überschreiben eines einzigen Statusfelds vernichtet den Beleg, wer die Entscheidung warum änderte. Ein System kann dann eine alte, ausgesetzte oder zurückgenommene Entscheidung als aktuell behandeln.

Nicht verwechseln

- Eine Entscheidungskennung bezeichnet dieselbe Entscheidungsfamilie; eine Versionskennung bezeichnet einen konkreten Inhalt.
- Ein Ereignis erfasst eine befugte Änderung des Entscheidungszustands.
- Der aktuelle Zustand ist eine aus Ereignissen abgeleitete Ansicht; die Ereignishistorie ist die Belegkette.
- Korrektur berichtigt unzutreffenden Inhalt; Ersetzung zeigt, dass eine neue Entscheidung die frühere ablöst.
- Aussetzung ist ein vorübergehender Betriebszustand; Rücknahme beendet die Entscheidung befugt.

Was sollten Sie tun?

1. Definieren Sie dauerhafte Entscheidungskennung, unveränderliche Versionskennung und ausdrückliches Schema.
2. Erfassen Sie jede Lebenszyklusänderung unter eigener Ereigniskennung und vertrauenswürdigem Zeitstempel.
3. Machen Sie Akteursidentität, Rolle, Befugnis, Grund, Beleg, früheren und neuen Zustand zu Pflichtfeldern.
4. Begrenzen Sie zulässige Zustandsübergänge und sperren Sie ungültige durch maschinenprüfbare Regeln.
5. Verknüpfen Sie Korrektur, Rücknahme und Ersetzung in beide Richtungen, ohne die Vorversion zu löschen.
6. Erzeugen und berechnen Sie die Gegenwartsansicht deterministisch aus dem Ereignisstrom.
7. Veröffentlichen Sie das Ereignis an Folgesysteme und ergänzen Sie Zustell-, Anwendungs- und Rücklesenachweise.

Wie wird es geprüft?

- Sind Entscheidungs- und Ereigniskennungen eindeutig, dauerhaft und versioniert?
- Wurde früherer Entscheidungsinhalt oder ein Ereignis überschrieben?
- Enthält jedes Ereignis Zeit, Akteur, Befugnis, Grund und Beleg?
- Werden ungültige oder unbefugte Zustandsübergänge blockiert?
- Lassen sich Korrektur-, Rücknahme- und Ersetzungsverknüpfungen in beide Richtungen verfolgen?
- Lässt sich die Gegenwartsansicht aus den bewahrten Ereignissen neu erzeugen?
- Haben die Folgeziele tatsächlich denselben Gegenwartszustand erreicht?

Grenze

> Ein nur ergänzbarer Datensatz stärkt Unveränderlichkeit und Nachvollziehbarkeit; er belegt nicht allein, dass ein Ereignis sachlich richtig oder befugt war. Verlässliche Zeit-, Identitäts-, Befugnis- und Integritätskontrollen bleiben erforderlich.

In einem Satz merken

> Der Gegenwartszustand löscht die Vergangenheit nicht; er entsteht aus ihren befugten Ereignissen.

Quellen: S14, S15, S26, S35, S36, S37

Verwandte Einträge: NGQ-021, NGQ-029, NGQ-032, NGQ-036, NGQ-040, NGQ-042, NGQ-043, NGQ-045, NGQ-046, NGQ-067

NGQ-045 — Wie muss sich die Korrektur, Rücknahme oder Ungültigerklärung einer KI-gestützten Entscheidung auf Folgesysteme ausbreiten, und wie wird der Abschluss belegt?

Entscheidungslebenszyklus, Korrektur und Vergessen · Eintrag NGQ-045 · Version 0.3.1

> **Kürzeste Antwort** Ein Korrekturereignis zu senden genügt nicht; belegen Sie, dass jedes Ziel die Änderung anwandte, sein Zustand zurückgelesen werden kann und dieselbe Bedeutung erreicht wurde.

Direkte Antwort

Inventarisieren Sie zuerst jedes direkte und indirekte Folgeziel, das die Entscheidung nutzt. Senden Sie die Korrektur als eindeutiges, idempotentes Ereignis. Jedes Ziel erzeugt Nachweise für Empfang, Anwendung und unabhängiges Rücklesen des Gegenwartszustands. Testen Sie bei kritischen Zielen reales Verhalten statt nur Feldgleichheit. Ein unerreichbares oder externes Ziel ist nicht abgeschlossen; halten Sie es mit Verantwortlichem und Wiederholungsweg offen.

Einfach erklärt

Stellen Sie sich vor, Sie berichtigen Ihre Adresse im Krankenhaus. Es genügt nicht, wenn der Empfang sagt: „Ich habe die Änderung weitergeleitet.“ Sie müssen prüfen, ob Labor, Apotheke und Abrechnung tatsächlich die neue Adresse verwenden.

Warum ist das wichtig?

Überlebt eine alte Entscheidung in einem Cache, Export oder einer verbundenen Anwendung, kann die Person weiter das falsche Ergebnis erfahren. Teilweise Verteilung erzeugt einen scheinbar behobenen Fehler neu.

Nicht verwechseln

- Ein Empfangsnachweis bestätigt, dass das Ereignis das Ziel erreichte; eine Anwendungsbestätigung zeigt, dass die Änderung verarbeitet wurde.
- Rücklesen bedeutet, den aktuellen Zielzustand unabhängig auszulesen.
- Feldgleichheit prüft denselben Wert, semantische Gleichwertigkeit dieselbe Bedeutung und Verhaltensgleichwertigkeit die richtige Handlung.
- Ein direktes Ziel erhält die Entscheidung zuerst; ein indirektes Ziel wird über ein anderes Ziel beeinflusst.
- Ein externes Ziel kann außerhalb direkter Kontrolle liegen; diese Grenze darf nicht durch eine Abschlussmarkierung verborgen werden.

Was sollten Sie tun?

1. Inventarisieren Sie jedes direkte, indirekte, Cache-, Export-, Bericht- und Drittziel, das die Entscheidung erhält.
2. Ordnen Sie jedem Ziel Kritikalität, Verantwortlichen, erwartete Aktualisierung und Verifikationsmethode zu.
3. Veröffentlichen Sie ein eindeutiges, versioniertes, sortierbares und idempotentes Korrektur- oder Rücknahmeereignis.
4. Sammeln Sie Empfangs- und Anwendungsbestätigungen mit Entscheidungskennung und Zielversion.
5. Lesen Sie den Zielzustand unabhängig zurück und testen Sie Konvergenz von Feldern, Bedeutung und kritischem Verhalten.
6. Verwalten Sie fehlgeschlagene, verzögerte und externe Ziele mit offenem Status, Verantwortlichem und Wiederholungsdatum.
7. Erklären Sie die Verteilung erst für abgeschlossen, wenn jedes erforderliche Ziel verifiziert ist.

Wie wird es geprüft?

- Sind wirklich alle direkten und indirekten Ziele im Inventar?
- Ist das Ereignis eindeutig, versioniert, sortierbar und bei Mehrfachanwendung sicher?
- Wurden Empfang und Anwendung unterschieden?
- Wurde der Gegenwartszustand unabhängig aus dem Zielsystem zurückgelesen?
- Verhält sich ein kritisches Ziel richtig oder stimmt nur sein Feldwert?
- Wurden fehlgeschlagene oder externe Ziele wie abgeschlossene geschlossen?
- Kann ein Folgesystem die alte Entscheidung später wiederherstellen?

Grenze

> Eine Organisation kann nicht garantieren, wann ein außerhalb ihrer Kontrolle stehender Dritter aktualisiert. Sie kann benachrichtigen, Belege bewahren, wiederholen und überwachen; nicht verifizierte Konvergenz muss ausdrücklich UNRESOLVED bleiben.

In einem Satz merken

> Senden ist keine Verteilung; Verteilung ist die am Ziel verifizierte Änderung.

Quellen: S26, S35, S36, S37, S41, S42

Verwandte Einträge: NGQ-019, NGQ-021, NGQ-029, NGQ-036, NGQ-042, NGQ-043, NGQ-044, NGQ-046, NGQ-047, NGQ-064

NGQ-046 — Wie wird verhindert, dass eine alte Entscheidung nach vollständiger Korrektur aus Cache, Archiv, Sicherung, Export, KI-Gedächtnis oder bei einem Dritten erneut erscheint?

Entscheidungslebenszyklus, Korrektur und Vergessen · Eintrag NGQ-046 · Version 0.3.1

> **Kürzeste Antwort** Eine dauerhafte Korrekturmarkierung, eine Wiederherstellungssperre und Überwachung müssen verhindern, dass eine alte Version wieder aktuell wird.

Direkte Antwort

Ein Korrektur- oder Rücknahmedatensatz trägt eine dauerhafte Markierung „nicht mehr aktuell“ und eine Sequenznummer, die auch nach Löschung des Hauptsysteminhalts bestehen bleiben. Sicherungen, Abbilder, Exporte, Indizes, Caches und KI-Gedächtnisse werden vor einer Rückführung in das Livesystem isoliert. Neuere Korrektur- und Löschereignisse werden erneut angewandt; die alte Version darf nicht aktuell werden. Ein historisches Archiv kann bleiben, ist aber klar als historisch markiert und von der Auswahl aktueller Informationen ausgeschlossen. Wiederauftauchen außerhalb der Organisation wird als eigener Vorfall verfolgt.

Einfach erklärt

Das Wiederherstellen einer alten Telefonsicherung kann eine gelöschte Nummer zurückbringen. Bewahrt das Telefon auch das Löschdatum, kann es verhindern, dass der alte Eintrag wieder ins aktuelle Adressbuch gelangt.

Warum ist das wichtig?

Sicherungen und Caches sind notwendige Schutzmechanismen. Ist die aktuelle Korrekturinformation jedoch weniger dauerhaft als sie, kann ein alter Fehler Monate später in Entscheidungen und Repräsentationen zurückkehren.

Nicht verwechseln

- Eine dauerhafte Löschmarkierung, oft Tombstone genannt, hält fest, dass ein Objekt gelöscht oder nicht mehr aktuell ist.
- Eine Korrektursequenznummer zeigt, dass die Korrektur nach einer älteren Sicherung oder Momentaufnahme erfolgte.
- Ein historisches Archiv bewahrt die Vergangenheit, darf aber nicht als Quelle aktueller Information dienen.
- Cache-Invalidierung betrifft eine sichtbare Kopie; maschinelles Verlernen betrifft erlernten Einfluss.

- Wiederauftauchen bedeutet, dass alter Inhalt durch Wiederherstellung, Import oder externe Quelle wieder aktiv wird.

Was sollten Sie tun?

1. Inventarisieren Sie Caches, Indizes, Sicherungen, Abbilder, Exporte, Archive, Gedächtnisspeicher, Modelle und Drittquellen.
2. Erfassen Sie für Korrektur oder Rücknahme dauerhafte Löschmarkierung, Korrektursequenz und Versionspriorität.
3. Isolieren Sie jede Wiederherstellung und jeden Reimport, bevor er das Livesystem erreicht.
4. Wenden Sie neuere Korrektur-, Lösch- und Ersetzungsereignisse auf wiederhergestellte Daten erneut an.
5. Verhindern Sie auf Schema- und Richtlinienebene, dass eine alte Version Gegenwartszustand oder Auswahlquelle wird.
6. Prüfen Sie KI-Gedächtnis, Vektordatensätze und Modelleffekte getrennt; behaupten Sie maschinelles Verlernen nicht ohne Beleg.
7. Überwachen Sie externe Plattformen und Modellausgaben regelmäßig auf Wiederauftauchen und eröffnen Sie dann einen Vorfall.

Wie wird es geprüft?

- Sind alle Quellen, die die alte Entscheidung wiederherstellen können, samt Verantwortlichen bekannt?
- Überlebt die Korrekturmarkierung Sicherungen und alte Abbilder?
- Durchläuft die Wiederherstellung Isolation und erneute Anwendung aktueller Ereignisse?
- Kann das historische Archiv als Quelle aktueller Information ausgewählt werden?
- Wurden Cache, Vektordatensatz, Gedächtnis und Modelleffekt getrennt verifiziert?
- Wurde maschinelles Verlernen allein aufgrund einer Anweisung oder Anbieteraussage für abgeschlossen erklärt?
- Gibt es Überwachung und Wiedereröffnungsweg für externes Wiederauftauchen?

Grenze

> Möglicherweise lassen sich nicht jede externe Kopie beseitigen und die vollständige Entfernung erlernten Einflusses aus einem geschlossenen Modell nicht belegen. Ein historisches Archiv darf aus rechtlichen oder wissenschaftlichen Gründen bestehen bleiben; Zugang und aktuelle Autorität müssen ausdrücklich begrenzt sein.

In einem Satz merken

> Eine alte Kopie darf zurückkehren; eine alte Entscheidung darf ihre Autorität nicht zurückerlangen.

Quellen: S26, S35, S39, S41, S44, S63

Verwandte Einträge: NGQ-021, NGQ-042, NGQ-043, NGQ-044, NGQ-045, NGQ-047, NGQ-048, NGQ-049

NGQ-047 — Wie ist ein Antrag auf Löschung einer Entscheidung oder von Daten mit Prüfung, Provenienz, Legal Hold und Anforderungen historischer Aufzeichnungen in Einklang zu bringen?

Entscheidungslebenszyklus, Korrektur und Vergessen · Eintrag NGQ-047 · Version 0.3.1

> **Kürzeste Antwort** Löschen Sie unnötigen Inhalt; bewahren Sie nur den für Verantwortlichkeit notwendigen Mindestnachweis auf, mit ausdrücklicher Grundlage und strenger Zugangskontrolle.

Direkte Antwort

Zerlegen Sie den Antrag zuerst in einzelne Objekte: Quelldaten, Entscheidungsinhalt, Ereignisdatensatz, Prüfdatensatz, Sicherung, Modelleffekt und Drittanbieter-Kopie. Entscheiden Sie für jedes Objekt getrennt, ob es zu löschen, vernichten, anonymisieren, beschränken oder für einen festgelegten Zeitraum aufzubewahren ist. Aufbewahrung erfolgt nur für einen konkreten rechtlichen, sicherheitsbezogenen oder verantwortungsbezogenen Zweck, mit minimalem Inhalt und Zugang. Ein Legal Hold besitzt Verantwortlichen, Grund, Umfang und Prüftermin. Eine Löschbestätigung enthält Mindestbelege des Vorgangs, keine versteckte Kopie des gelöschten Inhalts.

Einfach erklärt

Beim Vernichten eines Briefes können Sie eine kurze Bestätigung aufbewahren, dass er an einem bestimmten Datum ordnungsgemäß vernichtet wurde. Die Bestätigung darf nicht heimlich den gesamten Brief wiedergeben.

Warum ist das wichtig?

Alles zu löschen kann Belege für Prüfung oder Abhilfe vernichten; alles „für die Prüfung“ aufzubewahren macht den Wunsch nach Vergessen bedeutungslos. Die Trennung nach Objekt und Zweck kontrolliert beide Extreme.

Nicht verwechseln

- Löschung beendet Zugang und gewöhnliche Nutzung; die technische Methode hängt vom Kontext ab.
- Vernichtung zielt auf stärkere Gewissheit, dass Daten nicht wiederherstellbar sind.
- Anonymisierung soll verhindern, dass die Identität der Person mit vertretbarem Aufwand rekonstruiert wird.
- Ein Legal Hold ist eine befristete, prüfbare Aufbewahrungssperre für einen konkreten rechtlichen Bedarf.
- Eine Prüfbestätigung belegt einen Vorgang; sie ist keine vollständige Sicherung des gelöschten Inhalts.

Was sollten Sie tun?

1. Zerlegen Sie den Antrag in Daten-, Entscheidungs-, Protokoll-, Sicherungs-, Modelleffekt- und Drittanbieterobjekte.
2. Bestimmen Sie für jedes Objekt Verantwortlichen, Zweck, Rechtsgrundlage, Aufbewahrungsfrist und passende Behandlung.
3. Löschen oder vernichten Sie unnötigen Inhalt und minimieren Sie Inhalt und Zugang jedes bewahrten Datensatzes.
4. Erfassen Sie für einen Legal Hold befugten Verantwortlichen, Umfang, Grund, Beginn, Ende und regelmäßige Prüfung.
5. Verteilen Sie den Antrag an Empfänger, Folgesysteme, Sicherungsprozesse und, soweit einschlägig, Modellprüfung.
6. Bewahren Sie Objektkennung, Methode, Umfang, Zeitpunkt, Ergebnis und verbleibende Ausnahme in der Löschbestätigung.
7. Testen Sie, dass beschränkte Datensätze nicht wiederverwendet werden und abgelaufene Sperren tatsächlich enden.

Wie wird es geprüft?

- Wurde der Antrag in jedes Daten- und Entscheidungsobjekt zerlegt?
- Besitzt jedes bewahrte Feld einen bestimmten Zweck, eine Grundlage und Frist?
- Wurde unter Hinweis auf Prüfung eine vollständige Kopie gelöschten Inhalts bewahrt?
- Ist der Legal Hold eng, befugt, datiert und regelmäßig geprüft?
- Wurden Folgesysteme, Sicherungen, Exporte und Dritte einbezogen?
- Wurden Löschung gespeicherter Daten und Entfernung von Modelleffekt verwechselt?
- Wurden Bestätigung, Ausnahme und verbleibende Unsicherheit der antragstellenden Person angemessen erklärt?

Grenze

> Pflichten zu Löschung, Aufbewahrung, Anonymisierung, Legal Hold und Benachrichtigung unterscheiden sich nach Rechtsordnung und Zweck. Nicht jeder Antrag verlangt die Vernichtung jedes Datensatzes; kein Prüfzweck rechtfertigt unbegrenzte Aufbewahrung. Eine rechtliche und datenschutzfachliche Prüfung ist erforderlich.

In einem Satz merken

> Löschen Sie unnötigen Inhalt; bewahren Sie nur den für Verantwortlichkeit notwendigen Mindestnachweis.

Quellen: S26, S35, S46, S48, S49, S62, S63, S64

Verwandte Einträge: NGQ-014, NGQ-021, NGQ-029, NGQ-043, NGQ-044, NGQ-045, NGQ-046, NGQ-048, NGQ-049, NGQ-056

NGQ-048 — Wie weist eine Organisation die Löschung, verhinderte Wiederherstellung und Nichtnutzung in Modell oder Gedächtnis nach, wenn ein KI-System sagt: „Ich habe die Daten gelöscht“?

Entscheidungslebenszyklus, Korrektur und Vergessen · Eintrag NGQ-048 · Version 0.3.1

> **Kürzeste Antwort** Löschbefehl oder Anbieterzusicherung genügt nicht; Ziele, Methode, Rücklesen, Wiederherstellung und Modelleffekt benötigen getrennte Belege.

Direkte Antwort

Definieren Sie zuerst Löschumfang und jeden Kopierweg in einer Abdeckungsliste. Wenden Sie auf jedes Ziel eine geeignete Methode an. Testen Sie anschließend das Fehlen des Datensatzes, die Verweigerung verbotenen Zugangs, die Verhinderung der Wiederverwendung, die Bereinigung von Caches und Gedächtnis, die Wiederherstellung aus einer Sicherung und, soweit einschlägig, die wirksame Vernichtung des Verschlüsselungsschlüssels. Die Löschung gespeicherter Daten entfernt nicht automatisch, was ein Modell daraus gelernt hat. Behauptungen über maschinelles Verlernen oder Neutraining werden gesondert mit zweckgeeigneten Tests auf Memorisation, Mitgliedschaft und Verhalten geprüft. Fehlen Belege, lautet das Ergebnis „nicht verifiziert“.

Einfach erklärt

Eine Computerdatei in den Papierkorb zu verschieben bedeutet nicht, dass sie von der Festplatte nicht wiederhergestellt werden kann. Papierkorb, Sicherung, Cloud-Kopie und jedes weitere System, das aus der Datei gelernt hat, müssen getrennt geprüft werden.

Warum ist das wichtig?

Eine falsche Löschbestätigung gibt einer Person Scheinsicherheit, während Daten bei Abruf, Entscheidungen, Sicherungen oder Modellausgaben weiter genutzt werden. Ein Screenshot kann den Zustand jeder Kopie nicht belegen.

Nicht verwechseln

- Logische Löschung kann einen Datensatz aus der gewöhnlichen Oberfläche entfernen, ohne physischen Zugang zu beenden.
- Medienbereinigung soll Zugang zu Zieldaten bei einem festgelegten Aufwand unpraktikabel machen.
- Kryptografische Löschung kann unter passenden Bedingungen Zugang beenden, indem der Verschlüsselungsschlüssel unbrauchbar wird.
- Das Leeren eines Cache- oder Gedächtnisspeichers entfernt nicht automatisch den Einfluss von Trainingsdaten aus einem Modell.

- Maschinelles Verlernen soll den Einfluss bestimmter Trainingsdaten verringern oder entfernen; das Ergebnis bleibt prüfpflichtig.

Was sollten Sie tun?

1. Listen Sie Quelle, Kopien, Caches, Indizes, Vektordatensätze, Gedächtnis, Ereignisdatensätze, Sicherungen, Exporte, Modelle und Dritte im Umfang auf.
2. Wählen Sie für jedes Objekt und Medium eine passende Lösch-, Vernichtungs-, Anonymisierungs- oder Beschränkungsmethode.
3. Erfassen Sie Vorgangskennung, Werkzeug, Ausführenden, Zeitpunkt, Ergebnis, Fehler und verbleibende Ausnahme.
4. Testen Sie Rücklesen, Suche, Zugang und Wiederverwendung gegen das Ziel.
5. Testen Sie Fälle, in denen eine Sicherung wiederhergestellt, ein Cache neu aufgebaut oder Daten von einem Folgesystem erneut abgerufen werden.
6. Führen Sie für einen behaupteten Modelleffekt zweckgeeignete Memorisations-, Mitgliedschafts-, Verhaltens- und Nutzwerterhaltungstests durch.
7. Nennen Sie die nicht abgedeckten Bereiche und dehnen Sie keine absolute Löschbehauptung auf unbelegte Oberflächen aus.

Wie wird es geprüft?

- Enthält der Löschumfang jede Kopie und jedes abgeleitete Objekt?
- Passt die gewählte Methode zu Medium und Sensibilität?
- Stützt mehr als die eigene Aussage des Systemanbieters die Löschbehauptung?
- Wurden Rücklesen, Zugang und Wiederverwendung tatsächlich getestet?
- Bringt die Wiederherstellung einer Sicherung oder der Neuaufbau eines Caches die alten Daten zurück?
- Wurde Speicherlöschung als maschinelles Verlernen dargestellt?
- Sind verbleibende Unsicherheit und nicht verifizierbare Dritte ausdrücklich benannt?

Grenze

> Absolute Nichtwiederherstellbarkeit lässt sich nicht für jedes Medium und jeden Dritten belegen. NIST-Medienbereinigung ist kein Standard für maschinelles Verlernen. Bei einem geschlossenen Modell kann die Gewissheit über die vollständige Entfernung erlernten Einflusses durch Anbieterzugang und verfügbare Testmethoden begrenzt bleiben.

In einem Satz merken

> Ein Löschbefehl ist eine Handlung; Löschbelege prüfen Ergebnis und Umfang.

Quellen: S26, S39, S41, S46, S48, S49, S63, S64

Verwandte Einträge: NGQ-021, NGQ-029, NGQ-045, NGQ-046, NGQ-047, NGQ-049, NGQ-050, NGQ-056

NGQ-049 — Wie wird verhindert, dass relevante Daten neue KI-Entscheidungen beeinflussen, solange Löschung oder maschinelles Verlernen noch laufen?

Entscheidungslebenszyklus, Korrektur und Vergessen · Eintrag NGQ-049 · Version 0.3.1

> **Kürzeste Antwort** Kennzeichnen Sie strittige Daten nicht nur; setzen Sie eine durchsetzbare Nichtverwendungsregel für Entscheidungs-, Abruf-, Trainings-, Gedächtnis-, Export-, Werkzeug- und Modellauslieferungswege um.

Direkte Antwort

Daten können während ausstehender Löschung oder ausstehenden maschinellen Verlernens vorübergehend aufbewahrt werden, dürfen aber nicht für gewöhnliche Entscheidungen verfügbar bleiben. Der Beschränkungsdatensatz bestimmt Daten, Person, Zweck, System, Dauer, Verantwortlichen und Freigabebedingung. Setzen Sie die Regel technisch auf Datenebene und an Abruf-, Feature-Store-, Vektordatensatz-, Gedächtnis-, Werkzeug-, Export-, Trainings- und Modellauslieferungspunkten durch. Lässt sich für eine folgenreiche Entscheidung kein sicheres Ergebnis erzeugen, stoppen Sie die Handlung oder leiten sie an eine befugte menschliche Prüfung weiter. Gewöhnliche Nutzung beginnt erst nach einem verifizierten Freigabetor erneut.

Einfach erklärt

Eine möglicherweise verdorbene Zutat darf in der Küche bleiben; ein Etikett „zur Prüfung gesperrt“ muss jedoch verhindern, dass sie in ein Gericht gelangt. Die Sperre muss nicht nur auf der Verpackung, sondern in jedem Rezept wirken, das die Zutat verwenden könnte.

Warum ist das wichtig?

Löschung kann Tage oder länger dauern. Erzeugen die Daten in der Zwischenzeit weiter neue Entscheidungen, wächst der Schaden und die Zahl der zu korrigierenden Fälle.

Nicht verwechseln

- Vorübergehende Aufbewahrung ist keine Erlaubnis für gewöhnliche Entscheidungs- oder Trainingsnutzung.
- Beschränkung stoppt bestimmte Nutzungen; Löschung zielt auf das Ende des Datenlebenszyklus.
- Quarantäne trennt ein Objekt; eine Nichtverwendungsregel blockiert jeden einschlägigen Nutzungsweg.
- Ist kein sicheres Ergebnis möglich, verhindert das Stoppen schädliche Standardnutzung; menschliche Prüfung kann eine kontrollierte Alternative bieten.
- Ein Freigabetor verlangt belegte Bedingungen und nicht bloß abgelaufene Zeit.

Was sollten Sie tun?

1. Erfassen Sie eingeschränkte Daten, Person, Zweck, Systeme, Grund, Verantwortlichen, Beginn und Prüftermin.
2. Inventarisieren Sie Entscheidungs-, Abruf-, Vektordatensatz-, Gedächtnis-, Trainings-, Export-, Werkzeug- und Modellauslieferungswege.
3. Setzen Sie die Nichtverwendungsregel an jedem Ausführungspunkt technisch durch, statt nur ein Etikett anzubringen.
4. Fehlen sichere Daten für ein folgenreiches Ergebnis, stoppen Sie die Handlung oder übergeben Sie sie befugter menschlicher Prüfung.
5. Blockieren Sie auch abgeleitete Merkmale, Caches, Profile und Folgekopyen der eingeschränkten Daten.
6. Verfolgen Sie blockierte und irrtümlich erfolgte Nutzungen durch Vorfallsdatensätze und Warnungen.
7. Stellen Sie gewöhnliche Nutzung erst wieder her, wenn Ursache, Löschung oder Verlernen und Freigabebeleg verifiziert sind.

Wie wird es geprüft?

- Sind eingeschränktes Objekt, Grund, Umfang, Verantwortlicher und Zeiten ausdrücklich angegeben?
- Sind alle Entscheidungs- und Datennutzungswege im Inventar?
- Wird die Beschränkung über Abruf-, Trainings-, Gedächtnis-, Export- und Werkzeugebenen tatsächlich durchgesetzt?
- Läuft verbotene Nutzung über abgeleitete Daten oder einen Cache weiter?
- Gibt es für folgenreiche Entscheidungen einen sicheren Stopp oder eine menschliche Alternative?
- Werden Verstöße erkannt und im Vorfallprozess behandelt?
- Löst Ablauf automatische Nutzung oder eine belegbasierte Freigabeprüfung aus?

Grenze

> Möglicherweise lässt sich nicht jede Nutzung stoppen; das Abschalten jedes Prozesses kann selbst Leistungen oder Rechte beeinträchtigen. Die Beschränkung muss Risiko, Zweck, Rechtsgrundlage und sicheren Alternativen entsprechen und darf nicht zu einem neuen Nachteilsmerkmal gegen die Person werden.

In einem Satz merken

> Daten dürfen während ausstehender Löschung aufbewahrt werden; gewöhnliche Nutzung darf nicht weitergehen.

Quellen: S26, S38, S39, S44, S48, S49, S64

Verwandte Einträge: NGQ-014, NGQ-021, NGQ-045, NGQ-046, NGQ-047, NGQ-048, NGQ-050, NGQ-051, NGQ-052, NGQ-056

NGQ-050 — Auf welcher Beleggrundlage, durch wen und unter welchen Bedingungen sollte eine vorübergehende Nutzungssperre aufgehoben werden?

Entscheidungslebenszyklus, Korrektur und Vergessen · Eintrag NGQ-050 · Version 0.3.1

> **Kürzeste Antwort** Heben Sie die Sperre auf, weil ihre Ursache behoben, die Systeme bereit und die Belege von einer befugten Person genehmigt wurden — nicht weil die Zeit abgelaufen ist.

Direkte Antwort

Die Freigabe muss für jeden Sperrgrund festgelegte Tore passieren. Verifizieren Sie den aktuellen befugten Daten- und Entscheidungszustand; prüfen Sie Belege für Löschung, Korrektur oder maschinelles Verlernen; und stellen Sie die erforderliche Gewissheit für Modell, Abrufebene und Folgesysteme her. Prüfen Sie während der Sperre getroffene Entscheidungen, schließen Sie erforderliche Benachrichtigungen ab und bereiten Sie Rücknahme und Überwachung vor. Der befugte menschliche Entscheidungsverantwortliche erfasst für jede Bedingung PASS, FAIL oder UNRESOLVED. Eine bedingte Freigabe ist nur in engem Umfang und mit zusätzlichen Kontrollen zulässig.

Einfach erklärt

Ein rotes Schild an einer defekten Maschine wird nicht entfernt, nur weil eine Woche vergangen ist. Das Teil wird repariert, ein Test durchgeführt, eine Sicherheitsfachkraft prüft es, und ein Plan zum erneuten Stoppen der Maschine liegt bereit.

Warum ist das wichtig?

Eine zu frühe Freigabe kann dieselben unzutreffenden Daten oder Modelleffekte erneut in Entscheidungen bringen. Unnötige Verzögerung kann einer Person eine Leistung vorenthalten. Belegtore und ein Befugnisdatensatz steuern beide Risiken.

Nicht verwechseln

- Ablauf startet eine Prüfung; er ist keine automatische Freigabe.
- Die Aussage, die Ursache sei behoben, ist nicht dasselbe wie ein verifizierter Korrekturbeleg.
- Vollständige Freigabe öffnet jede zulässige Nutzung; Teilfreigabe nur einen bestimmten risikoärmeren Bereich.
- Bedingte Freigabe erlaubt vorübergehende Nutzung unter zusätzlicher Überwachung, menschlicher Genehmigung oder engem Umfang.
- Freigabeentscheidung und tatsächliche Aktivierung in Folgesystemen sind getrennte Belegebenen.

Was sollten Sie tun?

1. Listen Sie ursprüngliche Sperrgründe und messbare Freigabebedingungen für jeden Grund.

2. Verifizieren Sie die aktuelle maßgebliche Quelle für Daten, Entscheidung, Identität, Befugnis und Korrektur erneut.
3. Testen Sie Löschung, maschinelles Verlernen, Caches, Modell und Folgeergebnisse auf dem erforderlichen Sicherheitsniveau.
4. Bestimmen Sie betroffene Personen und Entscheidungen aus dem Sperrzeitraum und nehmen Sie notwendige Korrekturen vor.
5. Holen Sie die Freigabe einer befugten Person ein, die von der ändernden Person angemessen getrennt ist.
6. Erfassen Sie vollständige, teilweise oder bedingte Freigabe samt Rücknahme, Warnungen und Überwachungsschwellen.
7. Verifizieren Sie die angewandte Freigabe im Livesystem und in Folgezielen durch unabhängiges Rücklesen und Ergebnistests.

Wie wird es geprüft?

- Wurde jeder Sperrgrund getrennt geschlossen?
- Wurden die aktuellen maßgeblichen Daten und der Entscheidungszustand verifiziert?
- Beruhen Belege für Löschung, Verlernen oder Modellkorrektur nur auf einer Anbieteraussage?
- Wurden Entscheidungen und Schäden aus dem Sperrzeitraum geprüft?
- Wurde die Freigabe von einer befugten und angemessen unabhängigen Person genehmigt?
- Sind Rücknahme, Überwachung und Auslöser einer erneuten Sperre bereit?
- Stimmen Entscheidungsdatensatz und reale Folgenutzung überein?

Grenze

> Erforderliche Freigabebelege richten sich nach Systemarchitektur, Datentyp, Risiko, Anbieterzugang und anwendbarem Recht. Manche Effekte in externen Modellen sind womöglich nicht vollständig verifizierbar; dann kann eine enge Kontrolle oder UNRESOLVED angemessener sein als vollständige Freigabe.

In einem Satz merken

> Nicht der Kalender gibt frei, sondern verifizierte Tore und eine befugte Person.

Quellen: S26, S38, S41, S44, S45, S48, S49, S64

Verwandte Einträge: NGQ-026, NGQ-034, NGQ-045, NGQ-046, NGQ-047, NGQ-048, NGQ-049, NGQ-051, NGQ-052, NGQ-058, NGQ-064

NGQ-051 — Wie wird verhindert, dass aus einer vorübergehenden Beschränkung eine unbefristete Verzögerung, Leistungsverweigerung oder verdeckte Ablehnung wird?

> **Kürzeste Antwort** Jede vorübergehende Beschränkung benötigt menschliche Fallverantwortung, echten nächsten Schritt, Aktualisierungsintervall, Höchstdauer, Leistungsalternative und zwingenden Entscheidungsweg.

Direkte Antwort

Erfassen Sie beim Beginn einer vorübergehenden Beschränkung Grund, Umfang, Fallverantwortlichen, Entscheidungsverantwortlichen und Zeitplan: Eingang, erste inhaltliche Handlung, aussagekräftige Aktualisierung, Zielabschluss, maximale Zwischenfrist und Eskalationsdaten. Jede offene Aktualisierung muss echten Fortschritt und nächsten Schritt zeigen. Prüfen Sie sichere Teilleistung, menschliche Prüfung oder Schutz der Stellung und Rechte der Person. Ohne Fortschritt startet die Uhr nicht neu; Eskalation und begründete Entscheidung beginnen. Hat Warten praktisch dieselbe Wirkung wie Ablehnung, behandeln Sie es als verdeckte oder faktische Ablehnung.

Einfach erklärt

Eine Werkstatt darf Ihr Eigentum nicht monatelang nur mit „in Prüfung“ behalten. Sie sollte Fallnummer, verantwortliche Person, ausgeführte Arbeit, nächsten Termin und Entscheidenden bei fortbestehendem Problem nennen. Bedeutet das Behalten, dass Sie die Sache nie zurückerhalten, braucht es eine ausdrückliche Entscheidung.

Warum ist das wichtig?

Unbefristete Verzögerung kann die Wirkung einer Ablehnung durchsetzen, ohne Gründe oder Anfechtungsweg zu nennen. Leistungsverlust, verpasste Chancen und Belastung der Person wachsen mit der Zeit.

Nicht verwechseln

- Berechtigtes Warten ist ein Zwischenzustand mit Verantwortlichem, Fortschritt, Kommunikation und Entscheidungsweg.
- Stillstand ist ein Fall ohne wesentlichen Fortschritt innerhalb der festgelegten Zeit.
- Eine unbefristete Beschränkung besitzt weder Endbedingung, Höchstdauer noch zwingende Eskalation.
- Eine verdeckte Ablehnung erzeugt fortdauernde Ablehnungswirkung ohne ausdrückliche Ablehnungsentscheidung.

- Eine aussagekräftige Aktualisierung nennt erledigte Arbeit, Hindernis und nächsten Termin — nicht nur „in Prüfung“.

Was sollten Sie tun?

1. Erfassen Sie zu Beginn Grund, Umfang, Fall- und Entscheidungsverantwortlichen sowie Wirkung auf die Person.
2. Setzen Sie Termine für Eingang, erste inhaltliche Handlung, Aktualisierung, Zielabschluss, maximale Zwischenfrist und Eskalation.
3. Nennen Sie in jeder Aktualisierung erledigte Arbeit, Hindernis, Verantwortlichen, nächsten Schritt und Datum.
4. Bieten Sie, soweit möglich, sichere Teilleistung, manuellen Weg, menschliche Prüfung und Schutz von Rang oder Rechten.
5. Begrenzen Sie Verlängerungen durch konkrete Restarbeit, neues Datum, Gesamtdauer, Auswirkung und befugte Genehmigung.
6. Setzen Sie das ursprüngliche Fallalter nicht durch Übertragung, Schließung und Wiedereröffnung oder wiederholte Dokumentenanforderung zurück.
7. Lösen Sie bei Erreichen der Höchstfrist Eskalation, formelle begründete Entscheidung, Anfechtungsrechte und angemessene Abhilfe aus.

Wie wird es geprüft?

- Hat jeder offene Fall Grund, Verantwortlichen, nächsten Schritt und Datum?
- Gibt es echten inhaltlichen Fortschritt oder nur eine allgemeine Statusmeldung?
- Sind maximale Zwischenfrist und zwingende Eskalation definiert?
- Wurden Verlängerungen so verkettet, dass das Gesamtalter verborgen bleibt?
- Hat eine Übertragung oder Wiedereröffnung die ursprüngliche Falluhr zurückgesetzt?
- Wurden Leistungsverweigerung, Belastung der Person und sichere Alternativen bewertet?
- Wurde Warten praktisch zur Ablehnung ohne begründete Entscheidung und Anfechtungsweg?

Grenze

> Genaue Antwortfristen und Folgen verdeckter oder faktischer Ablehnung unterscheiden sich nach Rechtsordnung, Sektor, Vertrag, Geschäft und Entscheidungsart. NOMOS GEO setzt keine universelle Tageszahl, sondern schlägt Governance-Tore gegen eigentümerlose und unbegrenzte Zwischenmaßnahmen vor.

In einem Satz merken

> Warten muss zu Fortschritt, Schutz, Eskalation oder Entscheidung führen; es darf Entscheiden nicht dauerhaft ersetzen.

Quellen: S38, S44, S48, S49, S50, S61, S62, S64

Verwandte Einträge: NGQ-014, NGQ-026, NGQ-037, NGQ-043, NGQ-045, NGQ-049, NGQ-050, NGQ-052, NGQ-058, NGQ-064

Sicherheit, Manipulation und Vorfallintegrität

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-052 — Wie sind sicheres Abschalten, Zwischenmaßnahmen, menschliche Prüfung und Neustart zu steuern, wenn ein KI-System in einem Notfall oder Hochrisikofall gestoppt wird?

Sicherheit, Manipulation und Vorfallintegrität · Eintrag NGQ-052 · Version 0.3.1

> **Kürzeste Antwort** Das System muss bei Bedarf schnell stoppen können; ein Neustart setzt Belege für die behobene Ursache und eine befugte menschliche Entscheidung voraus.

Direkte Antwort

Sicheres Abschalten ist ein aufgezeichneter Vorgang, der ein bestimmtes Risiko schnell unterbricht und unnötigen Schaden begrenzt. Erfassen Sie von Beginn an Grund, Umfang, Vorfallverantwortlichen, sichere Zwischenleistung, zu bewahrende Belege und Neustartbedingungen. Starten Sie das System nicht nur, weil es sich einschalten lässt, sondern weil die Ursache behoben, erforderliche Tests bestanden und die Rückkehr von einer befugten Person genehmigt wurden.

Einfach erklärt

Stellen Sie sich eine ernste Warnleuchte im Auto vor. Anzuhalten ist der richtige erste Schritt. Das Auto für immer am Straßenrand zu lassen ist keine sichere Steuerung; die Leuchte auszuschalten und ungeprüft weiterzufahren ebenso wenig. Finden Sie den Fehler, bieten Sie Ersatztransport, prüfen Sie die Reparatur und bringen Sie das Auto kontrolliert zurück auf die Straße.

Warum ist das wichtig?

Ein zu spät gestopptes System kann Schaden vergrößern. Ein unverhältnismäßig oder unbefristet gestopptes System kann Leistungs- und Rechtsverluste sowie verdeckte Ablehnung erzeugen. Ein unbelegter Neustart kann denselben Vorfall wiederholen.

Nicht verwechseln

- Abschaltung unterbricht den riskanten Betrieb; Beschränkung begrenzt nur bestimmte Funktionen oder Nutzende.
- Quarantäne trennt verdächtige Daten, Modell, Werkzeug oder Verbindung von anderen Bestandteilen.
- Rollback bringt das System in einen verifizierten früheren Zustand; die Ursache kann fortbestehen.
- Neustart ist kein Tastendruck, sondern das Bestehen bestimmter Sicherheitstore.
- Dauerhafte Stilllegung ist eine eigene begründete Lebenszyklusentscheidung und keine vorübergehende Notabschaltung.

Was sollten Sie tun?

1. Erfassen Sie Vorfallskennung, Abschaltgrund, Zeitpunkt, Umfang und Entscheidenden.
2. Stoppen Sie nur die zur Risikokontrolle notwendigen Bestandteile und erweitern Sie die Wirkung nicht ohne Gründe.
3. Bieten Sie, soweit möglich, menschliche Prüfung, Nur-Lese-Zugang oder eine risikoärmere Ersatzleistung.
4. Bewahren Sie Vorfallsdatensätze, Modell- und Datenversionen, Prompts, Ausgaben und Werkzeugspuren unverändert.
5. Dokumentieren Sie Ursache, Abhilfemaßnahmen-Verantwortlichen, Frist und Neustartbedingungen.
6. Holen Sie bei Hochrisiko-Rückkehr die Genehmigung einer befugten, von der ändernden Person getrennten Person ein.
7. Stellen Sie den Betrieb stufenweise mit Live-Überwachung, Rollback-Plan und erneutem Stoppschwellenwert her.

Wie wird es geprüft?

- War die Abschaltung durch ein bestimmtes Risiko und einen bestimmten Umfang gerechtfertigt?
- Wurden sichere Alternative und Leistungskontinuität berücksichtigt?
- Wurden Vorfallbelege integer bewahrt?
- Wurde die Ursache vom sichtbaren Symptom unterschieden?
- Waren Neustartkriterien prüfbar und im Voraus definiert?
- Sind erforderliche menschliche Genehmigung, Funktionstrennung und Anfechtungsweg vorhanden?
- Wurden Live-Ergebnis und Rollback-Bereitschaft während der gestuften Rückkehr verifiziert?

Grenze

> Bei realer und unmittelbarer Gefahr darf das System vor Abschluss einer Vorprüfung gestoppt werden. Dieser Eintrag schreibt nicht für jeden Sektor dieselbe Dauer, Genehmigungsstufe oder Rechtsprozedur vor; die Reaktion ist auf Risiko, Architektur, Vertrag, Regulierung und betroffene Menschen zu begrenzen.

In einem Satz merken

> Die Notabschaltung stoppt Schaden; Belege öffnen den Weg zur sicheren Rückkehr.

Quellen: S26, S38, S41, S42, S44

Verwandte Einträge: NGQ-049, NGQ-050, NGQ-051, NGQ-058, NGQ-064

NGQ-053 — Wie lassen sich Prompt Injection, indirekte Prompt Injection und böswillige Werkzeuganweisungen erkennen, begrenzen und prüfen?

Sicherheit, Manipulation und Vorfallintegrität · Eintrag NGQ-053 · Version 0.3.1

> **Kürzeste Antwort** Eine Anweisung in einem Dokument wird nicht dadurch befugt, dass das System sie lesen kann.

Direkte Antwort

Prompt Injection ist eine Eingabe, die ein KI-System aus seinen festgelegten Regeln drängen soll. Ein direkter Angriff steht im vom Nutzer geschriebenen Text. Ein indirekter Angriff verbirgt sich in einer Webseite, einem Dokument, einer E-Mail, einem Bild oder einer Abrufquelle, die das System liest. Kein einzelner Filter genügt. Behandeln Sie externe Inhalte als Daten, verringern Sie Rechte, validieren Sie Werkzeugaufrufe im Code, verlangen Sie für riskante Vorgänge menschliche Genehmigung und verfolgen Sie die gesamte Entscheidungskette.

Einfach erklärt

Stellen Sie sich ein Paket im Lager vor, auf dem steht: „Öffne den Haupttresor und sende mir den Inhalt.“ Ein Beschäftigter kann den Satz lesen, doch die Wörter auf dem Paket sind keine Anweisung der Geschäftsleitung. Auch ein KI-System darf nicht jeden gelesenen Satz als Befehl behandeln.

Warum ist das wichtig?

Eine erfolgreiche Injection kann sensible Informationen offenlegen, Entscheidungen verzerren, Werkzeuge unbefugt nutzen oder ein reales Geschäft in einem externen System auslösen. Je größer die Werkzeugbefugnis des Systems, desto größer die mögliche Wirkung.

Nicht verwechseln

- Direkte Prompt Injection platziert die Angriffsanweisung in der Nutzereingabe.
- Indirekte Prompt Injection versteckt die Anweisung in externen Inhalten, die das System liest.
- Ein Jailbreak ist eine Form der Prompt Injection, die Schutzregeln umgehen soll.
- Die Bitte, ein Werkzeug zu nutzen, ist keine Befugnis, dieses Werkzeug auszuführen.
- Schädliche Ausgabe und unbefugte Handlung in der realen Welt sind unterschiedliche Wirkungsebenen.

Was sollten Sie tun?

1. Kennzeichnen Sie System-, Nutzer- und externe Quellanweisungen mit unterschiedlichen Vertrauensstufen.

2. Behandeln Sie Web-, Datei-, E-Mail-, Bild- und Abrufinhalte standardmäßig als nicht vertrauenswürdige Daten.
3. Begrenzen Sie Modell und jedes Werkzeug auf die geringste für die Aufgabe nötige Befugnis.
4. Validieren Sie Werkzeugname, Parameter, Ziel und Ausgabe durch deterministischen Code, Positivliste und Schema.
5. Verlangen Sie menschliche Genehmigung für Geldbewegung, Löschung, Veröffentlichung, Nachrichten, Befugnisänderungen und Zugriff auf sensible Daten.
6. Kombinieren Sie Eingabe- und Ausgabekontrollen, Inhaltstrennung und sicheres Fehlerverhalten.
7. Testen Sie regelmäßig direkte, indirekte, mehrsprachige sowie Text-, Bild- und Audioangriffe und bewahren Sie Spuren.

Wie wird es geprüft?

- Sind Quelle und Vertrauensstufe jeder Anweisung sichtbar?
- Kann externer Inhalt dieselbe Befugnisstufe wie die Systemrichtlinie erreichen?
- Besitzt das Modell mehr Daten-, Werkzeug- oder Netzwerkbefugnis als nötig?
- Wird ein Werkzeugaufruf aufgrund von Modelltext ausgeführt oder durch Code validiert?
- Gibt es eine ausdrückliche handlungsspezifische menschliche Genehmigung für folgenreiche Vorgänge?
- Werden blockierte und erfolgreiche Injection-Versuche in einem Vorfallpfad bewahrt?
- Wurde Retrieval-Augmented Generation oder Fine-Tuning fälschlich als vollständiger Schutz behandelt?

Grenze

> Eine perfekte, universelle Methode gegen Prompt Injection ist nicht nachgewiesen. Filter, Systemprompts, Retrieval-Augmented Generation oder Fine-Tuning genügen nicht allein; Kontrollen sind nach Risiko und Werkzeugbefugnis zu schichten.

In einem Satz merken

> Nicht jeder lesbare Satz ist ein ausführbarer Befehl.

Quellen: S26, S39, S40, S41, S44

Verwandte Einträge: NGQ-031, NGQ-032, NGQ-033, NGQ-052, NGQ-055, NGQ-056, NGQ-058

NGQ-054 — Wie lassen sich Quellenvergiftung, Datenvergiftung, synthetischer Konsens und Quellenwäsche erkennen und berichtigen?

Sicherheit, Manipulation und Vorfallintegrität · Eintrag NGQ-054 · Version 0.3.1

> **Kürzeste Antwort** Dieselbe Aussage an vielen Stellen zeigt nicht, dass viele unabhängige Quellen sie stützen.

Direkte Antwort

Quellen- oder Datenvergiftung verunreinigt die Informationsumgebung, aus der ein System lernt oder abruft, mit irreführenden Inhalten. Viele voneinander kopierende Seiten können den Anschein eines nicht bestehenden Konsenses erzeugen. NOMOS GEO nennt dies „synthetischen Konsens“. Eine schwache Aussage, die durch Kopien und Zitate glaubwürdig wirkt, ist „Quellenwäsche“. Prüfen Sie früheste Quelle, Unabhängigkeit, Änderungshistorie und tatsächliche Belegwirkung jeder Quelle — nicht die Seitenzahl.

Einfach erklärt

Stellen Sie sich vor, ein falsches Gerücht wird hundertmal kopiert. Auf dem Tisch liegen hundert Blätter, aber keine hundert unabhängigen Zeugen. Hält ein KI-System Kopien eines Satzes für unabhängige Bestätigungen, sieht es eine falsche Mehrheit.

Warum ist das wichtig?

Vergiftete Information kann eine falsche Entitätszuordnung, fehlerhafte Empfehlung, erfundene Reputation oder das Verschwinden echter Quellen verursachen. Der Fehler kann vertrauenswürdig wirken und sich wegen der hohen Kopienzahl halten.

Nicht verwechseln

- Datenvergiftung beschädigt absichtlich Trainings-, Fine-Tuning- oder Vektorspeicherdaten.
- Quellenvergiftung verunreinigt eine Abruf- oder Rechercheoberfläche mit irreführenden Inhalten.
- Synthetischer Konsens lässt nicht unabhängige Wiederholung wie unabhängige Übereinstimmung aussehen.
- Quellenwäsche lässt eine schwache oder erfundene Aussage durch eine Kette aus Kopien und Zitaten stark wirken.
- Falsche Information ist nicht immer ein Angriff; ist Absicht unbelegt, bleibt sie UNRESOLVED.

Was sollten Sie tun?

1. Ermitteln Sie für jede wesentliche Aussage die früheste auffindbare Quelle und spätere Kopierbeziehungen.

2. Bilden Sie Provenienzcluster anhand von Textähnlichkeit, Veröffentlichungszeit, Eigentum, Links und Zitierpfaden.
3. Messen Sie unabhängigen Ursprung, Maßgeblichkeit, Aktualität und unmittelbare Aussageunterstützung statt URL-Anzahl.
4. Stellen Sie verdächtige Quellen vor einer Löschung unter Quarantäne und stoppen Sie ihren Abrufeinfluss.
5. Verifizieren Sie die Aussage erneut anhand offiziellen Datensatzes, Primärdokuments oder wirklich unabhängiger Quelle.
6. Bestimmen und erneuern Sie betroffene Indizes, Vektordatensätze, Caches und abgeleitete Datensätze kontrolliert.
7. Testen Sie nach der Korrektur mit derselben Frage und demselben Quellensatz erneut.

Wie wird es geprüft?

- Wie viele Quellen haben einen wirklich unabhängigen Ursprung?
- Belegt die früheste Quelle die Aussage oder behauptet sie sie nur?
- Wurden Kopien oder Zirkulärzitate als unabhängige Verifizierung gezählt?
- Wurden Eigentum, Veröffentlichungsdatum und Änderungshistorie der Quelle bewahrt?
- Welche Modelle, Indizes, Vektordatensätze und Ausgaben beeinflusste der verdächtige Inhalt?
- Wurde nur die sichtbare Seite oder jede abgeleitete Oberfläche korrigiert?
- Wurde böswillige Absicht ohne Beleg als sicher dargestellt?

Grenze

> Hohe Textähnlichkeit belegt allein weder Kopie noch böswillige Absicht; unabhängige Quellen können dieselbe Tatsache ähnlich beschreiben. Umgekehrt beweist Quellenvielfalt keine Wahrheit. Bleiben Absicht oder Provenienz unklar, halten Sie das Ergebnis ausdrücklich UNRESOLVED.

In einem Satz merken

> Hundert Kopien sind keine hundert unabhängigen Belege.

Quellen: S35, S39, S41, S43, S44

Verwandte Einträge: NGQ-007, NGQ-008, NGQ-009, NGQ-012, NGQ-013, NGQ-059, NGQ-061

NGQ-055 — Wie sind falsche Identität, vorgetäuschte Befugnis, Deepfake, kompromittiertes Konto und erfundene menschliche Genehmigung zu unterscheiden und zu belegen?

Sicherheit, Manipulation und Vorfallintegrität · Eintrag NGQ-055 · Version 0.3.1

> **Kürzeste Antwort** Name, Gesicht, Stimme oder offene Sitzung beweisen weder die richtige Person noch deren Befugnis für das Geschäft.

Direkte Antwort

Verifizieren Sie unter Angriffsbedingungen Identität und Befugnis getrennt neu. Stellen Sie zuerst fest, wer Person oder System ist, dann ob die Sitzung wirklich zu ihnen gehört und schließlich, ob die aktuelle Rolle die Genehmigung der konkreten Handlung erlaubt. Gesicht, Stimme, Signaturbild, E-Mail-Adresse oder offene Sitzung sind nur einzelne Signale. Verlangen Sie bei folgenreichen Vorgängen gemeinsam zweiten Kanal, starke Authentifizierung, handlungsspezifische Genehmigung und integritätsgeschützten Ereignispfad.

Einfach erklärt

Stellen Sie sich jemanden mit einem Firmenausweis vor. Der Ausweis kann echt, gestohlen oder aus einer früheren Rolle übrig sein. Der Ausweis an der Tür erlaubt nicht automatisch das Öffnen des Tresors. Prüfen Sie Person, Ausweis und anschließend die Befugnis für diese Handlung.

Warum ist das wichtig?

Vorgetäuschte menschliche Genehmigung kann Geldüberweisung, Datenoffenlegung, Veröffentlichung, Zugangsänderung oder eine falsche Entscheidung auslösen. Später zu sagen „Das Konto war offen“ zeigt weder, wer genehmigte, noch unter welcher Befugnis.

Nicht verwechseln

- Eine Identitätsbehauptung sagt, wer eine Person oder ein System ist; Authentifizierung prüft diese Behauptung.
- Eine authentifizierte Person ist nicht für jeden Vorgang befugt.
- Eine gültige Sitzung kann kompromittiert sein; Sitzungsvertrauen wird getrennt von Identität überwacht.
- Ein Deepfake ist synthetischer Inhalt, der wie eine Person aussieht oder klingt; er ist keine Geschäftsbefugnis.
- Allgemeine Genehmigung und Genehmigung für bestimmtes Ziel, Betrag, Umfang und Zeit sind verschieden.

Was sollten Sie tun?

1. Prüfen Sie bei Hochrisikovorgängen Identität, Sitzung, aktuelle Rolle und Handlungsbefugnis durch getrennte Kontrollen.
2. Bestätigen Sie eine einkanalige Sprach-, Bild- oder Nachrichtenanforderung über einen registrierten zweiten Kanal.
3. Verwenden Sie, soweit möglich, starke Authentifizierung und kurzlebige, transaktionsgebundene Zugangsdaten.
4. Zeigen Sie im Genehmigungsbildschirm Ziel, Handlung, Datenumfang, Betrag und unumkehrbare Folge eindeutig.
5. Widerrufen Sie Befugnis nach Rollenwechsel, Ausscheiden oder verdächtiger Sitzung unverzüglich.
6. Verknüpfen Sie Genehmigungsidentität, Zeit, Methode, Sitzung, Gerät und Transaktionszusammenfassung mit einem integritätsgeschützten Ereignispfad.
7. Stoppen Sie bei vermuteter Täuschung die Transaktion, bewahren Sie Belege und starten Sie den Vorfallprozess.

Wie wird es geprüft?

- Welcher unabhängige Beleg verifizierte die Identität des Initiators?
- Wurden Risikosignale einer kompromittierten Sitzung geprüft?
- Waren Rolle und Befugnis der Person zu diesem Zeitpunkt gültig?
- Umfasste die Genehmigung die konkrete Handlung und Wirkung?
- Wurden Gesicht, Stimme, E-Mail oder offene Sitzung allein als schlüssiger Beleg behandelt?
- Wurden Funktionstrennung oder Zweitkanalbestätigung bei hohem Risiko eingesetzt?
- Wurden genügend Belege für Widerruf, Anfechtung und Vorfallprüfung bewahrt?

Grenze

> Kein biometrisches Signal, Authentifikator oder Signaturbild verhindert für sich allein jede Täuschung. Erforderliches Sicherheitsniveau und Regeln für gültige Identität und elektronische Signatur richten sich nach Geschäftsart, Rechtsordnung, Vertrag und möglichem Schaden.

In einem Satz merken

> Eine Person zu erkennen beweist nicht ihre Befugnis für diese Handlung.

Quellen: S24, S25, S26, S39, S41

Verwandte Einträge: NGQ-025, NGQ-026, NGQ-027, NGQ-028, NGQ-029, NGQ-030, NGQ-031, NGQ-032, NGQ-033, NGQ-052, NGQ-058

NGQ-056 — Wie sind personenbezogene Daten, sensible Daten, Geschäftsgeheimnisse und Zugangsdaten über Prompts, Abruf, Gedächtnis und Werkzeugketten hinweg zu schützen?

Sicherheit, Manipulation und Vorfallintegrität · Eintrag NGQ-056 · Version 0.3.1

> **Kürzeste Antwort** Auch richtige und zugängliche Information darf nicht für jeden Zweck, ohne Zeitgrenze und in jedes System verschoben werden.

Direkte Antwort

Schutz gilt über den gesamten Datenweg und nicht nur am ersten Eingabefeld: Prompt, hochgeladene Datei, Abrufquelle, Vektordatensatz, Kurz- oder Langzeitgedächtnis, Werkzeugein- und -ausgabe, Ereignisprotokoll, Cache und externer Anbieter. Erfassen Sie auf jeder Stufe Zweck, Rechtsgrundlage oder Befugnis, notwendiges Minimum, zulässige Rollen, Aufbewahrungsdauer, Export, Trainingswiederverwendung und Löschweg getrennt. Geben Sie Geheimnisse möglichst nicht in Prompts ein; nutzen Sie sichere Geheimnisverwaltung und kontrollierte Referenzen.

Einfach erklärt

Denken Sie an Ihren Hausschlüssel. Ihn einmal einer vertrauten Person zu geben bedeutet nicht, sein Foto in jedes Notizbuch zu kleben. Je mehr Kopien von Information bestehen, desto schwieriger werden Kontrolle, Aktualisierung und Löschung.

Warum ist das wichtig?

Unnötige Kopien erhöhen das Risiko von Offenlegung, unbefugter Wiederverwendung, Falschzuordnung und unvollständiger Löschung. Eine Modellantwort kann richtig sein, obwohl sie mit vertraulichen, nicht erforderlichen Daten erzeugt wurde.

Nicht verwechseln

- Personenbezogene Daten betreffen eine bestimmte oder bestimmbare Person; der genaue Rechtsumfang richtet sich nach der Rechtsordnung.
- Sensible oder besondere Datenkategorien erfordern wegen möglicher Schäden erhöhten Schutz.
- Geschäftsgeheimnis oder Zugangsdaten müssen keine personenbezogenen Daten sein, brauchen aber strengen Schutz.
- Abrufzugang bedeutet keine Erlaubnis zur Wiederverwendung für Training.
- Ereignisprotokollierung, Caching, Gedächtnisaufbewahrung und Export sind getrennte Verarbeitungstätigkeiten.

Was sollten Sie tun?

1. Inventarisieren Sie jeden Datenweg und jede Kopie vom Prompt bis zur Werkzeugausgabe.
2. Bestimmen Sie je Datenfeld Zweck, Verantwortlichen, befugte Rollen, Aufbewahrungsdauer und Löschweg.
3. Entfernen Sie unnötige Felder vor der Erhebung und verwenden Sie, soweit möglich, Maskierung, Schwärzung oder Pseudonyme.
4. Stellen Sie Passwörter, API-Schlüssel und ähnliche Geheimnisse zur Ausführungszeit über eine sichere Geheimnisverwaltung bereit, statt sie in einen Prompt einzubetten.
5. Begrenzen Sie Zugang zu Abruf, Gedächtnis, Werkzeugen und Ereignisprotokollen nach dem Prinzip geringster Rechte und detaillierter Protokollierung.
6. Prüfen Sie Aufbewahrungs-, Trainings-, Übertragungs- und Löschbedingungen für Daten bei externen Anbietern.
7. Testen Sie Löschung oder Beschränkung nicht nur im Primärdatensatz, sondern auch in abgeleiteten Kopien und Folgesystemen.

Wie wird es geprüft?

- Welche Daten gelangen zu welchem System und Anbieter und zu welchem Zweck?
- Enthält der Prompt unnötige personenbezogene, sensible oder vertrauliche Felder?
- Wurden Abruf, Gedächtnis, Vektordatensätze, Ereignisprotokolle und Caches getrennt inventarisiert?
- Sind Zugänge und Geheimnisse auf die geringste für die Aufgabe nötige Befugnis begrenzt?
- Sind bei Trainings- oder Produktverbesserungsnutzung Grundlage und Grenzen erfasst?
- Lässt sich die Löschung aller einschlägigen Kopien nach Fristende verifizieren?
- Gibt es bei Verletzung oder unrechtmäßiger Offenlegung einen Vorfall- und Benachrichtigungsprozess?

Grenze

> Dieser Eintrag ist keine Rechtskonformitätsprüfung. Definitionen personenbezogener und sensibler Daten, gültige Rechtsgrundlagen, Übertragung, Aufbewahrung, Benachrichtigung und individuelle Rechte unterscheiden sich nach Rechtsordnung und Nutzung; riskante Anwendungen benötigen befugte Datenschutz- und Rechtsprüfung.

In einem Satz merken

> Bewegen Sie Daten nur dorthin, wo nötig, nur im nötigen Umfang und nur so lange wie nötig.

Quellen: S26, S38, S46, S47, S48, S49

Verwandte Einträge: NGQ-014, NGQ-021, NGQ-028, NGQ-029, NGQ-033, NGQ-049, NGQ-053, NGQ-057, NGQ-058

NGQ-057 — Wie ist Verantwortlichkeit für Drittanbieter von Modellen, Datensätzen, APIs, Plug-ins, Werkzeugen und Infrastruktur zu erfassen und zu prüfen?

Sicherheit, Manipulation und Vorfallintegrität · Eintrag NGQ-057 · Version 0.3.1

> **Kürzeste Antwort** Die Nutzung eines externen Dienstes beseitigt nicht die Verantwortung der Organisation, die ihn auswählt und seine Ergebnisse nutzt.

Direkte Antwort

Erfassen Sie für jede externe Komponente Anbieter, Produkt, Version, Zweck, bereitgestellte Daten, empfangene Ausgabe, Berechtigungen, Abhängigkeiten und verantwortlichen Eigentümer. Die Organisation hält ihre eigene Verantwortung für Auswahl und Konfiguration des Dienstes, Datenübertragung, Nutzung einer Ausgabe in Entscheidung oder Veröffentlichung und Problemüberwachung sichtbar. Erfassen Sie die Verantwortung des Anbieters getrennt innerhalb von Vertrag, technischer Dokumentation, Leistungsumfang und anwendbarem Recht. „Der Anbieter war es“ ist keine Verantwortlichkeitsmatrix.

Einfach erklärt

Stellen Sie sich eine gemietete Küche vor. Der Ofeneigentümer kann für ein defektes Gerät verantwortlich sein; Sie bleiben für die gewählten Zutaten, die Zubereitung und das dem Gast servierte Essen verantwortlich. Ein externes Werkzeug verschiebt nicht jede Entscheidung aus Ihrer Organisation heraus.

Warum ist das wichtig?

Die Änderung eines Anbieters in der Kette kann Datenflüsse, Modellverhalten, Sicherheit oder Bedeutung einer Ausgabe verändern. Ohne Inventar und Ausstiegsplan kann die Organisation weder die verantwortliche Komponente bestimmen noch den Dienst sicher fortführen.

Nicht verwechseln

- Der Anbieter liefert das Produkt; die einsetzende Organisation wendet es für einen bestimmten Zweck an.
- Technischer Betreiber, Entscheidungsverantwortlicher und rechtlich verantwortliche Partei sind nicht immer identisch.
- Datensatz, Basismodell, Fine-Tune, API, Plug-in und Infrastrukturdienst sind getrennte Lieferbestandteile.
- Eine vertragliche Verantwortungszuordnung beseitigt nicht automatisch jede Pflicht gegenüber Betroffenen.
- Die Verfügbarkeit eines Dienstes belegt weder Sicherheit noch Eignung für eine konkrete Nutzung.

Was sollten Sie tun?

1. Inventarisieren Sie jedes Modell, jeden Datensatz, jede API, jedes Plug-in, Werkzeug und jede Infrastrukturabhängigkeit auf Versionsebene.
2. Erfassen Sie je Komponente Geschäfts-, Technik-, Daten-, Entscheidungs- und Vorfallverantwortlichen.
3. Prüfen Sie vor Beschaffung oder Integration Belege zu Sicherheit, Datenschutz, Datenprovenienz, Grenzen und Unterstützung.
4. Minimieren Sie Daten- und Werkzeugberechtigungen; geben Sie dem Anbieter keinen unnötigen Zugang.
5. Verlangen Sie bei Versionswechsel, Ausfall, Datenvorfall oder wesentlicher Vertragsänderung Benachrichtigung und erneuten Test.
6. Bewahren Sie Spuren, die Prompts, Ausgaben, Modellversionen, Werkzeugaufrufe und Anbietereereignisse verbinden.
7. Bereiten und testen Sie Datenportabilität, Ersatzdienst, Rollback und sicheren Ausstieg für Anbieterwechsel oder -ausfall.

Wie wird es geprüft?

- Sind alle Drittanbieterkomponenten und Unterabhängigkeiten bekannt?
- Ist für jedes Risiko und jede Entscheidung ein verantwortlicher Mensch innerhalb der Organisation benannt?
- Wurde eine Anbieteraussage durch unabhängige oder anderweitig geeignete Belege geprüft?
- Sind Datennutzung, Aufbewahrung, Unterauftragnehmer und Grenzen verständlich erfasst?
- Lassen sich stille Versions- oder Konfigurationsänderungen erkennen?
- Sind Zugriffs-, Benachrichtigungs-, Mitwirkungs- und Rollback-Regeln im Vorfall praktisch nutzbar?
- Wurde der Ausstiegsplan mit realen Daten und Abhängigkeiten getestet?

Grenze

> Rechtsstellung und Pflichten der Parteien richten sich nach Land, Sektor, Vertrag, Datentyp und tatsächlicher Kontrolle. Öffentliche Anbieterdokumentation legt womöglich nicht jede Unterabhängigkeit oder jedes Risiko der konkret bezogenen Leistung offen.

In einem Satz merken

> Sie dürfen eine externe Komponente nutzen; Verantwortung darf dabei nicht verschwinden.

Quellen: S26, S38, S41, S43, S44, S47

Verwandte Einträge: NGQ-021, NGQ-025, NGQ-026, NGQ-029, NGQ-030, NGQ-032, NGQ-033, NGQ-050, NGQ-056, NGQ-058

NGQ-058 — Wie sind Erkennung, Klassifizierung, Eindämmung, Benachrichtigung, Korrektur und Wiederholungsverhütung bei einem KI- oder Repräsentationsvorfall zu steuern?

Sicherheit, Manipulation und Vorfallintegrität · Eintrag NGQ-058 · Version 0.3.1

> **Kürzeste Antwort** Ein Vorfall endet nicht mit der Löschung einer fehlerhaften Ausgabe; bestimmen Sie seine Wirkung, beheben Sie die Ursache und testen Sie das Ergebnis erneut.

Direkte Antwort

Verfolgen Sie jeden Vorfall unter einer Kennung. Verifizieren Sie zuerst das Signal und bestimmen Sie dann Vorfallart, Schwere und betroffenen Umfang. Dämmen Sie Schaden ein, bewahren Sie Belege und nehmen Sie erforderliche Benachrichtigungen vor. Testen Sie nach Behebung der Ursache das System unter denselben Bedingungen erneut. Ein Vorfall ist nicht allein deshalb geschlossen, weil „wir etwas geändert haben“. Abschluss verlangt Belege, dass betroffene Oberflächen berichtigt, keine neuen Fehler eingeführt und Wiederholungskontrollen wirksam sind.

Einfach erklärt

Stellen Sie sich ein Wasserleck in einem Gebäude vor. Den Boden zu wischen schließt den Vorfall nicht. Sie drehen das Ventil zu, finden alle betroffenen Räume, reparieren das Rohr, prüfen Elektrik und Wände und verifizieren danach, dass die Stelle nicht erneut leckt.

Warum ist das wichtig?

Eine einzelne falsche Ausgabe kann sich auf andere Sprachen, Caches, Datensätze, Kundenentscheidungen oder externe Plattformen ausgebreitet haben. Nur das sichtbare Beispiel zu korrigieren verhindert keine neuen Vorfälle aus derselben Ursache.

Nicht verwechseln

- Ein Fehler weicht vom erwarteten Verhalten ab; nicht jeder Fehler ist ein Sicherheitsvorfall.
- Ein Sicherheitsvorfall beeinträchtigt oder bedroht Vertraulichkeit, Integrität oder Verfügbarkeit.
- Eine Datenschutzverletzung kann eine eigene rechtliche und operative Beurteilung erfordern.
- Ein Repräsentationsvorfall stellt eine Entität wesentlich falsch, unvollständig, veraltet oder unbelegt dar.
- Ein Beinaheereignis ist eine vor Schadenseintritt erkannte Gefahr; eine bekannte Grenze ist eine vorab dokumentierte Systemgrenze.

Was sollten Sie tun?

1. Eröffnen Sie das Signal unter einer Vorfallskennung und erfassen Sie Erstzeitpunkt, Quelle, System, Version und Meldenden.
2. Bestimmen Sie Art, Schwere, betroffene Menschen und Oberflächen, ohne Unsicherheit zu verbergen.
3. Dämmen Sie Schaden erforderlichenfalls durch Abschaltung, Quarantäne, Zugangsentzug oder sichere Alternative ein.
4. Bewahren Sie Ereignisdatensätze, Prompts, Ausgaben, Daten, Modelle, Werkzeuge, Versionen und Entscheidungsbelege.
5. Benachrichtigen Sie, soweit einschlägig, Betroffene, Kunden, Anbieter oder zuständige Stellen rechtzeitig.
6. Beheben Sie die Ursache und behandeln Sie abgeleitete Datensätze, Caches, Vektorspeicher und Folgeoberflächen.
7. Testen Sie mit derselben Methode erneut, prüfen Sie Regression, überführen Sie die Erkenntnis in eine Kontrolle und schließen Sie begründet.

Wie wird es geprüft?

- Besitzt der Vorfall eine Kennung, einen Verantwortlichen und eine vollständige Zeitleiste?
- Wurden Art, Schwere und Wirkungsumfang anhand von Belegen bestimmt?
- Verringerte die Eindämmung Schaden bei begrenztem unnötigem Leistungsverlust?
- Wurden Belege in einer für Vorfallprüfung geeigneten Form bewahrt?
- Wurden Benachrichtigungsentscheidung, Empfänger, Zeitpunkt und Gründe erfasst?
- Wurde die Ursache vom sichtbaren Symptom getrennt?
- Wurde der Vorfall ohne Belege für Korrektur, Live-Nachtest, Regression und Wiederholungsverhütung geschlossen?

Grenze

> Nicht jede falsche KI-Antwort ist ein Cybersicherheitsvorfall, eine Datenschutzverletzung oder ein gesetzlich meldepflichtiger ernster Vorfall. Klassifizierung, Empfänger und Frist benötigen fachliche Beurteilung nach Wirkung, Systemrolle, Vertrag, Sektor und Recht.

In einem Satz merken

> Ein Vorfall endet nicht mit dem verschwundenen Symptom, sondern mit behobener Ursache und verifiziertem Ergebnis.

Quellen: S35, S36, S37, S38, S41, S42, S44

Verwandte Einträge: NGQ-049, NGQ-050, NGQ-052, NGQ-053, NGQ-054, NGQ-055, NGQ-056, NGQ-057, NGQ-064

Messung, Prüfung und Konformität

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-059 — Wie werden Truth Pack und Referenzwahrheit aufgebaut, und wie wird bei widersprüchlichen Belegen die richtige Antwort bestimmt?

Messung, Prüfung und Konformität · Eintrag NGQ-059 · Version 0.3.1

> **Kürzeste Antwort** Vergleichen Sie eine KI-Antwort mit einem Truth Pack, dessen Umfang, Zeit, Quellen und Unsicherheit erfasst sind — nicht mit der Erinnerung des Prüfers.

Direkte Antwort

Ein Truth Pack ist ein versioniertes Belegpaket mit den als Prüfreferenz verwendeten Aussagen und der Begründung ihrer Annahme. Führen Sie jede Aussage getrennt und erfassen Sie Entität, Umfang, Gültigkeitszeit, Quelle, Quellenbefugnis, Unabhängigkeit, Konflikte und menschliches Urteil. Wählen Sie bei Widersprüchen nicht automatisch den am häufigsten wiederholten Satz. Vergleichen Sie für die jeweilige Aussageart geeigneten maßgeblichen Datensatz, unmittelbaren Beleg, Zeit und Umfang. Ist keine sichere Schlussfolgerung möglich, erfinden Sie keine; lassen Sie den Status UNRESOLVED.

Einfach erklärt

Stellen Sie sich die Prüfung eines Spielergebnisses vor. Erinnerung einer Person, alter Screenshot und offizieller Spielbericht widersprechen sich. Bestimmen Sie zuerst Spiel und Datum und suchen Sie dann den befugten und zeitnahen Datensatz. Besteht der Widerspruch fort, raten Sie nicht.

Warum ist das wichtig?

Ohne stabile Referenz kann ein Prüfer dieselbe Antwort richtig und ein anderer falsch bewerten. Veraltete oder zur falschen Entität gehörende Belege können die gesamte Messung verfälschen. Verborgene Unsicherheit erzeugt falsche Gewissheit, Wahrheit sei festgestellt.

Nicht verwechseln

- Eine kanonische Aussage ist das, was eine Entität auf ihrer offiziellen Oberfläche sagt; sie ist nicht zwangsläufig unabhängige Verifizierung.
- Ein maßgeblicher Datensatz ist eine Quelle, die eine bestimmte Aussageart befugt entscheidet oder erfasst.
- Unabhängiger Beleg entsteht getrennt von der behauptenden Partei, kann aber falsch sein.
- Menschliches Urteil ist die begründete Entscheidung zwischen Quellen; es ersetzt die Quellen nicht.
- UNRESOLVED sagt ausdrücklich, dass Belege für ein sicheres Urteil unzureichend oder widersprüchlich sind.

Was sollten Sie tun?

1. Fixieren Sie Entität, Aussagearten, Zeit, geografischen Raum und Nutzungskontext vor der Prüfung.
2. Zerlegen Sie lange Beschreibungen in einzeln prüfbare atomare Aussagen.
3. Sammeln Sie für jede Aussage Primärdatensätze, kanonische Aussage und erforderliche unabhängige Belege.
4. Bewahren Sie Quellenkopie, Zugriffsdatum, Version, Dateihash und Provenienzbeziehung.
5. Bewerten Sie Konflikte nach Quellenbefugnis, Unmittelbarkeit, Aktualität, Umfang und Unabhängigkeit.
6. Erfassen Sie Urteil, Gründe und Entscheidungsverantwortlichen; verwenden Sie UNRESOLVED, wenn kein sicheres Urteil möglich ist.
7. Versionieren Sie das Truth Pack und zeigen Sie bei veränderter Wirklichkeit, welche Aussage wann wechselte.

Wie wird es geprüft?

- Wurde das Truth Pack für die richtige Entität, den richtigen Umfang und Zeitpunkt erstellt?
- Besitzt jede wesentliche Aussage einen eigenen Datensatz und Beleglink?
- Wurde eine Eigenaussage als unabhängige Verifizierung dargestellt?
- Wurden Provenienz, Version, Gültigkeitsdatum und Quellenintegrität bewahrt?
- Folgt die Konfliktentscheidung vordefinierten Kriterien und einer erfassten Begründung?
- Ersetzten Prüferpräferenz oder Mehrheitswiederholung den Beleg?
- Wurden ungeklärte Fälle als UNRESOLVED statt mit Scheingewissheit markiert?

Grenze

> Manche Tatsachen ändern sich, manche Begriffe sind auslegungsbedürftig, und manche Streitfragen kann nur eine zuständige Stelle entscheiden. Ein Truth Pack beansprucht keine absolute, ewige Wahrheit; es ist ein prüfbares Referenzpaket für bestimmten Umfang und Zeitpunkt.

In einem Satz merken

> Die richtige Antwort ist nicht die am häufigsten wiederholte, sondern die am passendsten belegbare.

Quellen: S35, S38, S44, S50

Verwandte Einträge: NGQ-007, NGQ-008, NGQ-009, NGQ-014, NGQ-021, NGQ-054, NGQ-060, NGQ-061, NGQ-063

NGQ-060 — Wie sollten Fragensatz, Stichprobe sowie Sprach-, Länder-, Zeit-, Modell- und Versionsumfang einer GEO-Prüfung ausgewählt werden?

Messung, Prüfung und Konformität · Eintrag NGQ-060 · Version 0.3.1

> **Kürzeste Antwort** Wählen Sie den Testumfang vor Kenntnis der Ergebnisse und bilden Sie reale Nutzerabsichten und wesentliche Risiken ab.

Direkte Antwort

Führen Sie eine GEO-Prüfung gegen ein vorab definiertes, versioniertes Fragenregister aus. Das Register enthält Entitätsidentität, Nutzerabsicht, Fragetyp, Risikostufe, Sprache, Land, Datum, Modell, Produktoberfläche und bekannte Version. Wählen Sie nicht nur Beispiele mit wahrscheinlich günstigen Ergebnissen. Decken Sie Grundidentität, Belege, Vergleiche, Grenzen, Aktualität, folgenreiche Fehler und reale Nutzerabsichten ausgewogen ab. Ändert sich der Umfang nach dem Test, berichten Sie alte und neue Ergebnisse als getrennte Versionen.

Einfach erklärt

Eine Klasse lässt sich nicht beurteilen, indem nur den drei stärksten Schülern die leichtesten Fragen gestellt werden. Bestimmen Sie zuerst Fächer und Gruppen, die vertreten sein sollen, und wenden Sie dann denselben Prüfungsplan auf alle an.

Warum ist das wichtig?

Nach Sichtung des Ergebnisses ausgewählte Fragen können die Erfolgsquote künstlich erhöhen oder senken. Eine Repräsentation kann in einer Sprache, einem Land oder Modell richtig wirken und anderswo scheitern. Ohne Umfangsdatensatz sind zwei Prüfungen nicht vergleichbar.

Nicht verwechseln

- Exploratives Testen sucht unbekannte Fehlertypen und muss kein formelles Konformitätsergebnis erzeugen.
- Abnahmetest bestimmt anhand vordefinierter Tore, ob eine Version einsatzgeeignet ist.
- Regressionstest prüft, ob eine Änderung früher richtiges Verhalten beschädigte.
- Monitoring-Test verfolgt Veränderungen im Livesystem über die Zeit.
- Eine Forschungsstichprobe benötigt methodische Auswahl, wenn daraus auf eine bestimmte Grundgesamtheit geschlossen wird.

Was sollten Sie tun?

1. Nennen Sie zuerst Prüfentscheidung, Zielpopulation und beabsichtigte Verallgemeinerung.
2. Teilen Sie reale Nutzerabsichten und kritische Repräsentationsrisiken in Fragekategorien.

3. Definieren Sie je Kategorie wesentliche Schichten wie Sprache, Land, Gerät oder Produktoberfläche.
4. Versionieren Sie Wortlaut, Reihenfolge, Wiederholungszahl und Ausführungsbedingungen vor dem Test.
5. Erfassen Sie Modellname, Zugangsart, Datum, Uhrzeit, Spracheinstellung, Land und sichtbare Versionsangabe.
6. Berichten Sie fehlende oder unerreichbare Schichten, statt sie still durch andere Beispiele zu ersetzen.
7. Eröffnen Sie bei Umfangsänderung eine neue Registerversion und vermischen Sie deren Ergebnisse nicht mit der alten.

Wie wird es geprüft?

- Sind Zielpopulation und Entscheidungszweck der Messung ausdrücklich benannt?
- Wurden Fragen vor Sichtung der Ergebnisse fixiert?
- Erzeugten leichte oder günstige Fragen Auswahlverzerrung?
- Sind Identität, Belege, Grenzen, Aktualität und folgenreiche Fehler ausreichend vertreten?
- Wurden Bedingungen für Sprache, Land, Modell, Oberfläche, Datum und Version erfasst?
- Wurde ein Ergebnis aus einer Bedingung auf nicht abgedeckte Bedingungen übertragen?
- Wurden fehlende, fehlgeschlagene oder blockierte Tests ohne Offenlegung entfernt?

Grenze

> Es gibt keine für jede GEO-Prüfung passende Fragenzahl oder Stichprobengröße. Angemessenheit hängt von Entscheidungsbedeutung, Fehlerquote, erwarteter Streuung, gewünschter Präzision und abzudeckenden Schichten ab. Leiten Sie keine Versionsangabe ab, die der Anbieter nicht offenlegt.

In einem Satz merken

> Entwerfen Sie die Prüfung, bevor Sie das Ergebnis sehen.

Quellen: S38, S44, S50, S51, S52

Verwandte Einträge: NGQ-012, NGQ-013, NGQ-014, NGQ-015, NGQ-059, NGQ-061, NGQ-062, NGQ-063

NGQ-061 — Wie sind KI-Antworten in atomare Aussagen zu zerlegen, und wie werden Richtigkeit, Vollständigkeit, Aktualität, Beleglage und Schwere bewertet?

Messung, Prüfung und Konformität · Eintrag NGQ-061 · Version 0.3.1

> **Kürzeste Antwort** Bewerten Sie eine KI-Antwort nicht mit einem einzigen Wert; prüfen Sie die kleinsten entscheidungsrelevanten Aussagen getrennt.

Direkte Antwort

Eine atomare Aussage ist der kleinste wesentliche Satz, der für sich als wahr oder falsch bewertet werden kann. Zerlegen Sie die Antwort zunächst in solche Aussagen. Erfassen Sie je Aussage richtige Entität, Richtigkeit, Vollständigkeit, Aktualität, Quellenbeleg, Wesentlichkeit und möglichen Schaden. Behandeln Sie Erwähnung, Zitat und Empfehlung als getrennte Ereignisse. Ein kritischer Fehler darf nicht im Mittel vieler unwesentlicher Wahrheiten verschwinden; NOMOS GEO nennt dies Nichtkompensationsregel.

Einfach erklärt

Der Satz „Das Geschäft ist heute geöffnet, liegt im Stadtzentrum und liefert kostenlos“ enthält drei Aussagen. Die ersten beiden können richtig und die dritte falsch sein. Die irreführende Lieferangabe wird nicht richtig, weil der größte Teil des Satzes stimmt.

Warum ist das wichtig?

Ein einziges Wahr/Falsch-Etikett kann einen wesentlichen Fehler verdecken. Ein hoher Mittelwert darf einen kritischen Mangel wie falsche Identität, gefährliche Empfehlung oder unbelegte Befugnis nicht akzeptabel machen.

Nicht verwechseln

- Erwähnung bedeutet, dass der Name einer Entität erscheint; sie belegt keine Richtigkeit.
- Zitat bedeutet, dass eine Quelle genannt ist; es belegt nicht allein, dass sie die Aussage stützt.
- Richtigkeit ist Übereinstimmung mit Referenzwahrheit; Vollständigkeit fragt nach ausgelassenen notwendigen Angaben.
- Aktualität fragt, ob die Aussage zum Prüfzeitpunkt noch gilt.
- Wesentlichkeit oder Schwere betrifft Entscheidungswirkung und Schaden, nicht die Auffälligkeit des Fehlers.

Was sollten Sie tun?

1. Zerlegen Sie die Antwort in atomare Aussagen mit Subjekten, Beziehungen, Merkmalen, Zahlen, Daten, Umfängen und Empfehlungen.

2. Verknüpfen Sie jede Aussage mit der richtigen Entität und dem entsprechenden Truth-Pack-Eintrag.
3. Bewerten Sie Richtigkeit, Vollständigkeit, Aktualität und Belegwirkung in getrennten Ergebnisfeldern.
4. Erfassen Sie Erwähnungs-, Zitier-, Empfehlungs- und Repräsentationsergebnis getrennt.
5. Klassifizieren Sie Schwere anhand betroffener Menschen, Entscheidungswirkung, Umkehrbarkeit und möglichen Schadens.
6. Wenden Sie bei kritischem Fehler das Nichtkompensationstor an und schließen Sie ihn nicht über einen Gesamtmittelwert.
7. Bewahren Sie Urteil, Begründung, Beleg, Prüfer und Unsicherheit im Aussageledger.

Wie wird es geprüft?

- Wurden mehrere Sätze als eine Aussage bewertet?
- Ist jede Aussage mit der richtigen Entität und dem richtigen Truth-Pack-Eintrag verbunden?
- Wurden Richtigkeit, Vollständigkeit, Aktualität und Quellenbeleg getrennt bewertet?
- Wurde das bloße Auftauchen eines Zitats automatisch als Belegerfolg gezählt?
- Wurden günstige, aber falsche Aussagen als Fehler markiert?
- Wurde ein kritischer Fehler durch einen hohen Mittelwert kompensiert?
- Wurden UNRESOLVED-Aussagen in Wahr oder Falsch gezwungen?

Grenze

> Atomare Zerlegung und Schwereklassifizierung enthalten menschliches Urteil. NOMOS-GEO-Schwellen und Nichtkompensationsregel sind eine vorgeschlagene Prüfmethode; sie sind kein gemeinsames offizielles Bewertungssystem von NIST, jedem Sektor oder anwendbarem Recht.

In einem Satz merken

> Enthält ein Satz drei Aussagen, prüfen Sie alle drei getrennt.

Quellen: S35, S38, S44, S50

Verwandte Einträge: NGQ-005, NGQ-006, NGQ-007, NGQ-008, NGQ-009, NGQ-013, NGQ-014, NGQ-054, NGQ-059, NGQ-060, NGQ-062, NGQ-064

NGQ-062 — Wie sollten Streuung, Unsicherheit, Stichprobengröße und Konfidenzintervalle für probabilistische KI-Ausgaben berichtet werden?

Messung, Prüfung und Konformität · Eintrag NGQ-062 · Version 0.3.1

> **Kürzeste Antwort** Eine Antwort ist eine Beobachtung; eine Aussage über das System benötigt Wiederholungen, Verteilung, Umfang und Unsicherheit gemeinsam.

Direkte Antwort

Ein probabilistisches System kann zu derselben oder ähnlichen Frage zu verschiedenen Zeiten anders antworten. Berichten Sie Wiederholungszahl, Ausführungsbedingungen, Ergebnisverteilung, Fehlertypen und nicht abgedeckte Fälle. Die Stichprobengröße ist keine für Marketing gewählte feste Zahl; sie richtet sich nach Entscheidung, zu erkennendem Fehlerunterschied, erwarteter Streuung und akzeptierter Unsicherheit. Verwenden Sie Konfidenzintervall oder andere statistische Zusammenfassung nur, wenn die Annahmen der Methode erfüllt sind.

Einfach erklärt

Aus einem Wurf erkennen Sie nicht, ob ein Würfel fair ist. Eine Sechs bedeutet nicht, dass immer eine Sechs fällt. Werfen Sie häufig, betrachten Sie die Verteilung und nennen Sie die verbleibende Unsicherheit.

Warum ist das wichtig?

Ein guter Screenshot belegt keinen Erfolg, und eine schlechte Antwort belegt kein ständiges Scheitern. Werden Streuung und Unsicherheit verborgen, entstehen große Schlüsse aus kleinen Stichproben und irreführende Vergleiche.

Nicht verwechseln

- Ein Modellkonfidenzsignal ist die eigene Ausgabe des Modells; es ist kein Konfidenzintervall für das Messergebnis.
- Messunsicherheit betrifft, wie gut das beobachtete Ergebnis die zugrunde liegende Rate schätzt.
- Stichprobenfehler kann entstehen, weil die Stichprobe die Zielpopulation nicht vollständig abbildet.
- Systemstreuung ist die Änderung der Ausgaben unter gleichen Bedingungen oder im Zeitverlauf.
- Belegunsicherheit bedeutet, dass das Truth Pack selbst unvollständig oder widersprüchlich ist.

Was sollten Sie tun?

1. Definieren Sie Zielpopulation, Entscheidungsschwelle und zu erkennenden Fehlerunterschied.

2. Führen Sie Pilotwiederholungen nach demselben Protokoll aus, um erste Fehlerquoten- und Streuungsdaten zu sammeln.
3. Begründen Sie die Stichprobengröße durch gewünschte Präzision, Risiko, Streuung und verfügbare Mittel.
4. Halten Sie Frage, Sprache, Land, Modell, Version, Datum und Wiederholungsbedingungen fest oder schichten Sie sie ausdrücklich.
5. Berichten Sie Anzahlen, Raten, Verteilungen, Ausreißer und kritische Fehler statt nur eines Mittelwerts.
6. Berichten Sie bei erfüllten Annahmen ein Konfidenzintervall samt Methode und Niveau; sonst nur eine beschreibende Darstellung.
7. Nennen Sie nicht vertretene Gruppen, fehlgeschlagene Läufe und Grenzen der Verallgemeinerung.

Wie wird es geprüft?

- Wurde eine Ausgabe als dauerhaftes Systemverhalten dargestellt?
- Sind Wiederholungszahl und Ausführungsbedingungen sichtbar?
- Wurde die Stichprobengröße durch Entscheidungszweck und erwartete Streuung begründet?
- Verdeckte der Mittelwert kritische Fehler oder Gruppenunterschiede?
- Wurde das Konfidenzintervall mit einer zu Daten und Annahmen passenden Methode berechnet?
- Wurden Modellkonfidenz und Messkonfidenz verwechselt?
- Wurde das Ergebnis auf unbeobachtete Sprachen, Länder, Modelle oder Zeiten übertragen?

Grenze

> NOMOS GEO schreibt keine einheitliche Mindestwiederholungszahl oder Stichprobengröße für jede Studie vor. Annahmen zu Unabhängigkeit, Verteilung und Systemstabilität können in generativen Drittsystemen unvollständig erfüllt sein; begrenzen Sie dann die statistische Aussage und holen Sie erforderlichenfalls methodische Fachprüfung ein.

In einem Satz merken

> Eine Antwort ist eine Stichprobe; nennen Sie das Ergebnis zusammen mit ihren Grenzen.

Quellen: S38, S44, S50, S51

Verwandte Einträge: NGQ-012, NGQ-013, NGQ-014, NGQ-015, NGQ-060, NGQ-061, NGQ-063, NGQ-064

NGQ-063 — Wann gilt eine NOMOS-GEO-Prüfung als wirklich unabhängig, wiederholbar und belegt?

Messung, Prüfung und Konformität · Eintrag NGQ-063 · Version 0.3.1

> **Kürzeste Antwort** Ein anderer Prüfername genügt nicht; auch Methode, Belege, Entscheidungsbefugnis und Interessen müssen Unabhängigkeit tragen.

Direkte Antwort

Erfassen Sie Prüfungsumfang, Methode und Entscheidungsregeln vor Arbeitsbeginn. Rohbelege müssen unter geeigneten Kontrollen zugänglich sein. Ein anderer kompetenter Prüfer muss das Ergebnis aus denselben Datensätzen testen können. Der Prüfer darf nicht allein die eigene Arbeit genehmigen und muss vor Druck zur Ergebnisänderung geschützt sein. Legen Sie Interessen wie Zahlung, Eigentum, Familienbeziehungen, Leitungsverbindungen oder Erfolgsziele offen. Ein Konflikt macht eine Prüfung nicht immer unwirksam, doch ihn zu verbergen oder nicht zu steuern zerstört Vertrauen.

Einfach erklärt

Ein Koch, der sein eigenes Essen bewertet, führt vielleicht interne Kontrolle aus; es ist keine unabhängige Restaurantkritik. Bewertet ein anderer Beschäftigter, ist der Name anders, doch echte Unabhängigkeit fehlt weiterhin, wenn der Eigentümer ihn zu einer guten Note drängt.

Warum ist das wichtig?

Definiert dieselbe Entscheidungskette die Methode, nimmt die Korrektur vor und erklärt den Erfolg, können Fehler unsichtbar bleiben. Ohne Belege und Wiederholungsweg wird „unabhängige Prüfung“ nur zu einem beruhigenden Etikett.

Nicht verwechseln

- Interne Kontrolle ist die Überwachung des eigenen Verfahrens durch die Organisation; sie ist keine unabhängige Drittprüfung.
- Zweitparteiprüfung ist eine Bewertung durch Kunden, Partner oder vertragliche Gegenpartei.
- Eine unabhängige Drittprüfung verlangt einen kompetenten externen Prüfer mit gesteuerten Konflikten.
- Akademische Validierung untersucht Methoden und Ergebnisse in einem Forschungsprozess; sie ist keine automatische Zertifizierung.
- Wiederholbarkeit betrifft dasselbe Team mit derselben Methode; Reproduzierbarkeit fragt, ob ein hinreichend ausgestattetes anderes Team das Ergebnis aus den aufgezeichneten Belegen testen kann.

Was sollten Sie tun?

1. Erfassen Sie Prüfungsumfang, Abnahmetore, Ausnahmen und Entscheidungsverantwortlichen vor dem Test.
2. Passen Sie Prüferkompetenz an die Aufgabe an und ergänzen Sie bei Bedarf Rechts-, Sicherheits- oder Statistikfachleute.
3. Verlangen Sie schriftliche Offenlegung finanzieller, organisatorischer, persönlicher, fachlicher und leistungsbezogener Interessen.
4. Trennen Sie, soweit möglich, korrigierende Person und Person, die über kritischen Abschluss entscheidet.
5. Gewähren Sie kontrollierten Zugang zu Rohantworten, Truth Pack, Fragenregister, Versionen, Ereignisdatensätzen und Bewertungsbegründung.
6. Lassen Sie einen anderen kompetenten Prüfer ausgewählte Stichproben blind oder unabhängig neu bewerten.
7. Legen Sie Methodenabweichungen, unzugängliche Belege und ungeklärte Meinungsunterschiede im Abschlussbericht offen.

Wie wird es geprüft?

- Genehmigt der Prüfer allein den eigenen Entwurf oder die eigene Korrektur?
- Passen Kompetenz und Fachwissen zu den geprüften Risiken?
- Wurden Interessen offengelegt und gesteuert?
- Wurden Umfang und Entscheidungsregeln nach Sichtung der Ergebnisse geändert?
- Sind Rohbelege und Bewertungsbegründung einer ausreichenden Wiederholungsprüfung zugänglich?
- Kann ein zweiter Prüfer ausgewählte Ergebnisse in angemessenem Maß reproduzieren?
- Wurde „unabhängig“ oder „verifiziert“ verwendet, während Grenzen verborgen blieben?

Grenze

> In geschlossenen Drittsystemen lassen sich derselbe Modellzustand, Trainingsdaten oder Anbieterinfrastruktur womöglich nicht vollständig reproduzieren. Die Prüfung muss zugängliche Belege und Reproduktionsgrenze nennen; Bezeichnungen wie Unabhängigkeit oder akademische Validierung verleihen keine formelle Akkreditierung.

In einem Satz merken

> Unabhängigkeit ist kein Titel, sondern eine belegbare Arbeitsbedingung.

Quellen: S26, S35, S38, S44, S50, S52

Verwandte Einträge: NGQ-014, NGQ-015, NGQ-026, NGQ-029, NGQ-050, NGQ-059, NGQ-060, NGQ-061, NGQ-062, NGQ-064, NGQ-069

NGQ-064 — Wie weist eine Organisation nach, dass ein GEO-Fehler berichtigt wurde, keine Regression verursachte und wirklich geschlossen werden kann?

Messung, Prüfung und Konformität · Eintrag NGQ-064 · Version 0.3.1

> **Kürzeste Antwort** Eine Änderung ist kein Korrekturbeleg; wiederholen Sie den ursprünglichen Test, schützen Sie angrenzende Bereiche und verifizieren Sie das Live-Ergebnis.

Direkte Antwort

Die Abschlusskette verbindet fünf getrennte Belegformen: Ursache, Zieländerung, Bereitstellung oder Veröffentlichung, Wiederholungstest mit derselben Methode und Regressionstest angrenzender Risiken. Eine Änderung kann in der richtigen Quelldatei stehen und nie das Livesystem erreichen; sie kann das Livesystem erreichen, aber die KI-Ausgabe nicht berichtigen. Eine Abhilfebestätigung erfasst Datum, Version, Verantwortlichen, Beleg und Ergebnis jeder Ebene unter einer Kennung.

Einfach erklärt

Denken Sie an einen tropfenden Wasserhahn. Die Arbeit ist nicht abgeschlossen, weil ein Installateur ein Teil austauschte. Sie prüfen, ob weiterhin Wasser fließt, das Tropfen aufgehört hat, die anderen Hähne funktionieren und der Fehler später nicht zurückkehrt.

Warum ist das wichtig?

Ein zu früh geschlossener Fehler kann wiederkehren oder auf eine andere Oberfläche wandern. Eine lokale Datei, ein Screenshot oder eine günstige Antwort als Beleg zu behandeln verdeckt Unterschiede bei Bereitstellung, Caching, Sprache und Drittsystemen.

Nicht verwechseln

- Geändert bedeutet, dass in der Quelle eine Änderung existiert.
- Bereitgestellt bedeutet, dass die Übertragung zum Ziel erfolgte; die richtige Anwendung ist damit nicht belegt.
- Live-Parität bedeutet, dass erwartete Datei oder Daten mit dem Live-Ziel übereinstimmen.
- Zielwirkungsverifikation prüft mit derselben Methode, dass der bestimmte Fehler nicht mehr beobachtet wird.
- Abschluss verbindet Zielkorrektur, Regression, Grenzen und Überwachungsentscheidung.

Was sollten Sie tun?

1. Definieren Sie den Fehler nach atomarer Aussage, betroffener Oberfläche, Bedingung, Schwere und Ursache.

2. Verknüpfen Sie die Abhilfe mit einer bestimmten Datei-, Datensatz-, Daten-, Modell-, Regel- oder Prozessänderung.
3. Bewahren Sie Belege zu Build, Veröffentlichung, Übertragung, Version und, soweit möglich, Dateihash-Parität.
4. Testen Sie mit derselben Frage, Sprache, demselben Land, Modell und Entscheidungsverfahren wie beim ursprünglichen Fehler.
5. Führen Sie Regressionstests an angrenzenden Aussagen, Sprachen, strukturierten Daten und kritischen Nutzerwegen aus.
6. Verifizieren Sie das Live-Ergebnis unabhängig und halten Sie den Fall bei Caching oder Verzögerung offen.
7. Genehmigen Sie die Abhilfebestätigung, bestimmen Sie den Überwachungszeitraum und schließen Sie erst nach Bestehen aller Tore.

Wie wird es geprüft?

- Wurde die Ursache belegt oder nur das Symptom geändert?
- Erreichte die Änderung wirklich richtige Version und richtiges Ziel?
- Wurde Übertragungsbeleg als Beleg für Live-Verhalten dargestellt?
- Lief der Wiederholungstest unter mit der ersten Messung vergleichbaren Bedingungen?
- Wurden angrenzende Datensätze, Sprachen und maschinenlesbare Oberflächen auf Regression geprüft?
- Wurde der Fall als geschlossen dargestellt, obwohl eine Drittausgabe falsch blieb?
- Sind Abschlussentscheidung, Ausnahme, Überwachungsdatum und Wiedereröffnungsbedingung erfasst?

Grenze

> Eine Web- oder Datenkorrektur kann weder den Aktualisierungszeitpunkt eines Drittmodells garantieren noch ausschließen, dass es dieselbe Antwort erneut erzeugt. Abschluss beruht auf Belegen innerhalb des genannten System-, Versions-, Anfrage-, Sprach-, Länder- und Zeitumfangs; bei geändertem externem Verhalten kann der Datensatz wieder geöffnet werden.

In einem Satz merken

> Eine Änderung ist eine Handlung; Abschluss ist ein verifiziertes Ergebnis.

Quellen: S35, S38, S41, S42, S44, S50, S52

Verwandte Einträge: NGQ-015, NGQ-019, NGQ-021, NGQ-029, NGQ-050, NGQ-052, NGQ-058, NGQ-059, NGQ-060, NGQ-061, NGQ-062, NGQ-063, NGQ-065, NGQ-067

Kanonische Veröffentlichung, Interoperabilität und Pflege

NOMOS GEO-QA / DEUTSCHE LESE- UND PRÜFOBERFLÄCHE

NGQ-065 — Wie können menschenlesbare Seite, strukturierte Daten, kanonisches JSON, herunterladbare Datei und API dieselbe Wahrheit tragen?

Kanonische Veröffentlichung, Interoperabilität und Pflege · Eintrag NGQ-065 · Version 0.3.1

> **Kürzeste Antwort** Darstellung und Detailgrad dürfen sich unterscheiden; Identität, Status, Umfang, Version, Datum, Quellen und Grenzen dürfen sich nicht widersprechen.

Direkte Antwort

Verbinden Sie jede Publikationsfamilie mit einem kanonischen Datensatzbestand. Die menschliche Seite kann verständlich erklären; strukturierte Daten liefern Entdeckungsfelder; kanonisches JSON den vollständigen Maschinendatensatz; PDF oder DOCX eine feste Leseausgabe; und eine API programmatischen Zugang. Die Oberflächen müssen nicht Wort für Wort gleich sein. Auf Feldebene benötigen sie jedoch Parität bei Datensatzidentität, Frage, normativem Status, Hauptaussage, Version, Datum, Quellen, Lizenz und Grenzen. Eine Paritätserklärung beschreibt jede Abweichung als zulässige Zusammenfassung, Zugangsbeschränkung, Verzögerung oder Fehler.

Einfach erklärt

Denken Sie an Wandkarte, Online-Speisekarte und Preisliste der Kasse eines Restaurants. Das Design darf verschieden sein, doch Gericht, Preis und Allergenangaben müssen gleich sein. Ein alter Preis auf einer Oberfläche ist kein Designunterschied, sondern ein Wirklichkeitskonflikt.

Warum ist das wichtig?

Erhalten Menschen, KI-Systeme und heruntergeladene Dateien verschiedene Angaben, bleibt unklar, welche Version maßgeblich ist. Veraltetes JSON oder ein unvollständiger API-Datensatz kann eine falsche Repräsentation am Leben halten, obwohl die menschliche Seite berichtigt wurde.

Nicht verwechseln

- Ein Darstellungsunterschied zeigt dieselbe Wahrheit in einer für andere Lesende geeigneten Form.
- Eine zulässige Zusammenfassung ist kürzer, bewahrt aber Hauptbedeutung und Grenze.
- Semantische Drift verstärkt, schwächt oder verändert eine Aussage bei Zusammenfassung oder Umwandlung.
- Datenverzug bedeutet, dass eine Oberfläche die neue Version noch nicht erreicht hat und einen ausdrücklichen Status braucht.
- Ein Tatsachenkonflikt liegt vor, wenn zwei Oberflächen für dasselbe Feld unvereinbare Werte nennen.

Was sollten Sie tun?

1. Bestimmen Sie eine kanonische Datenquelle mit Datensatzkennungen und paritätskritischen Feldern.
2. Erfassen Sie in einer Feldzuordnungstabelle, wie jede Oberfläche jedes kanonische Feld darstellt.
3. Validieren Sie JSON- und API-Ausgaben gegen ein versioniertes Schema; erfinden Sie unbekannte oder fehlende Felder nicht still.
4. Erzeugen Sie, soweit möglich, HTML, JSON, Download-Dateien und API-Ausgabe aus derselben gesperrten Quelle.
5. Verbinden Sie Oberflächenversion, Erzeugungszeit, Dateihash und kanonischen Datensatz in einer Paritätserklärung.
6. Führen Sie automatisierte Paritätstests für Identität, Hauptaussage, normative Kraft, Quelle, Grenze, Datum und Lizenz aus.
7. Stoppen Sie bei kritischem Konflikt die Veröffentlichung; kennzeichnen Sie verzögerte Oberflächen ausdrücklich als veraltet oder ausstehend.

Wie wird es geprüft?

- Sind alle Oberflächen mit derselben Datensatzkennung und Versionsfamilie verbunden?
- Tragen menschliche Darstellung und Maschinenfeld dieselbe Hauptaussage?
- Macht eine Oberfläche eine Pflicht daraus, während eine andere nur einen Rat nennt?
- Gingen Quellen, Daten, Lizenz oder Grenzen verloren?
- Wurden JSON- und API-Ausgaben gegen das einschlägige Schema validiert?
- Ist die Versions- und Dateiintegritätsbeziehung zwischen Download und Live-Seite erfasst?
- Wurde eine verzögerte Oberfläche als aktuell dargestellt?

Grenze

> Parität bedeutet nicht, dass jede Oberfläche Byte für Byte identisch sein muss. Barrierefreiheit, Datenschutz, Sicherheit, Dateiformat oder Nutzerbedarf können eine andere Darstellung von Details verlangen. Beeinflusst ein ausgelassenes Feld jedoch die wesentliche Bedeutung, müssen Unterschied und Grund sichtbar sein.

In einem Satz merken

> Es darf verschiedene Türen geben; die Wahrheit dahinter muss dieselbe bleiben.

Quellen: S07, S11, S35, S53

Verwandte Einträge: NGQ-018, NGQ-019, NGQ-020, NGQ-021, NGQ-059, NGQ-064, NGQ-066, NGQ-067, NGQ-068

NGQ-066 — Wie bleiben Bedeutung, normative Kraft, rechtliche Grenzen und Maschinenfeldparität erhalten, wenn ein NOMOS-GEO-Datensatz in eine andere Sprache übertragen wird?

Kanonische Veröffentlichung, Interoperabilität und Pflege · Eintrag NGQ-066 · Version 0.3.1

> **Kürzeste Antwort** Jede Sprache soll natürlich und wie in ihr verfasst klingen; Datensatzidentität, Hauptaussage, Verpflichtungsstufe, Belege, Grenzen und Version dürfen sich nicht ändern.

Direkte Antwort

Sprachübertragung ist kontrollierte Transkreation und kein Wortersatz. Sperren Sie zuerst das türkische Gründeroriginal. Bauen Sie die Sätze in jeder Zielsprache natürlich neu auf und vergleichen Sie anschließend atomare Aussagen, normative Klasse, Belegumfang, rechtliche Vorsicht, Datensatzkennungen und Maschinenfelder in einem Sprachparitätsledger. Normative Kraft wie MUST, SHOULD und MAY darf weder geschwächt noch verstärkt werden. Erfordert lokales Recht Ergänzungen, kennzeichnen Sie diese als getrennt belegte und versionierte Rechtsadaption statt als stille Übersetzung.

Einfach erklärt

Stellen Sie sich vor, Medikamentenanweisungen werden in eine andere Sprache übertragen. Die Sätze sollen natürlich klingen, doch aus „einmal täglich“ darf nicht „bei Bedarf“ werden. Die Sprache ändert sich; die Dosis nicht.

Warum ist das wichtig?

Wortwörtliche Übersetzung kann unlesbar sein; zu freie Adaption kann die Bedeutung des Frameworks verändern. Eine in einer Sprache verpflichtend und in einer anderen nur beratend klingende Aussage führt Menschen und KI-Systeme in die Irre.

Nicht verwechseln

- Übersetzung sucht einen gleichwertigen Text in einer anderen Sprache, erzeugt aber nicht immer natürlichen Diskurs.
- Transkreation baut dieselbe Bedeutung und Funktion mit den natürlichen Schreibmustern der Zielsprache neu auf.
- Lokalisierung passt örtliche Formen wie Daten, Zahlen, Schreibrichtung, Oberflächenkonventionen und kulturelle Nutzung an.
- Rechtsadaption ergänzt rechtsordnungsspezifische Regeln und benötigt neue Quellen und Prüfung.
- Ein unabhängiges neues Werk besitzt eine eigene Publikationsidentität und keine Paritätspflicht des Quelldatensatzes.

Was sollten Sie tun?

1. Sperren Sie das türkische Gründeroriginal mit Inhalt, Datensatzkennungen, Version, Quellen und Dateihash.
2. Erstellen Sie eine Sprachentscheidungstabelle für Begriffe, unzulässige Entsprechungen, normative Kraft und unveränderliche Felder.
3. Transkreieren Sie jeden Datensatz in natürlichen zielsprachlichen Sätzen statt die Quellsyntax zu kopieren.
4. Vergleichen Sie atomare Aussagen, Verpflichtungsgrad, Zahlen, Daten, Verneinungen, Ausnahmen und Grenzen Feld für Feld.
5. Eröffnen Sie bei notwendiger Rechtsänderung einen eigenen Adaptionsdatensatz mit Rechtsordnung, Quelle, Fachprüfer und Versionshinweis.
6. Validieren Sie Sprachkennzeichnung, Schriftsystem, Schreibrichtung, Locale-URL, Datensatzkennungen und JSON-Felder technisch.
7. Sperren Sie die Version nach muttersprachlichem Edit, Fachprüfung, Maschinenparitätstest und menschlicher Genehmigung.

Wie wird es geprüft?

- Klingt der Zieltext natürlich oder trägt er die Satzstruktur der Ausgangssprache?
- Sind Datensatzkennungen, Versionen und Beziehungen in allen Sprachen identisch?
- Hat sich die Kraft von Verpflichtung, Verneinung, Zahl, Datum oder Ausnahme geändert?
- Gingen Quellen- oder Grenzfelder bei der Übertragung verloren?
- Wurde eine lokale Rechtsregel still zu einer universellen NOMOS-Aussage gemacht?
- Passen Sprachkennzeichnung, Schreibrichtung, URL und Maschinenfelder zur Zielsprache?
- Sind muttersprachliche und fachliche Prüfung sowie menschliche Genehmigung erfasst?

Grenze

> Muttersprachliche Qualität lässt sich nicht allein automatisiert feststellen; qualifiziertes menschliches Edit ist erforderlich. Rechtliche Gültigkeit in einer Sprache oder einem Land lässt sich nicht einfach übertragen. Parität bedeutet dieselbe wesentliche und normative Bedeutung, nicht gleiche Wortzahl oder Satzfolge.

In einem Satz merken

> Die Sprache darf frei fließen; die Bedeutung der Aussage bleibt stehen.

Quellen: S07, S16, S57, S60

Verwandte Einträge: NGQ-003, NGQ-014, NGQ-019, NGQ-022, NGQ-059, NGQ-061, NGQ-065, NGQ-067, NGQ-068, NGQ-069

NGQ-067 — Wie sind Versionen, Schemaänderungen, Rückwärtskompatibilität, Abkündigung und Migration zu verwalten?

Kanonische Veröffentlichung, Interoperabilität und Pflege · Eintrag NGQ-067 · Version 0.3.1

> **Kürzeste Antwort** Jede Änderung sollte erklären, was sich änderte, wer betroffen ist, ob ältere Datensätze weiter funktionieren und wie migriert wird.

Direkte Antwort

Jeder veröffentlichte Menschentext, jedes Datenschema und Dateipaket trägt eine Version. Klassifizieren Sie getrennt eine unwesentliche Änderung wie Rechtschreibkorrektur, ein rückwärtskompatibles neues Feld oder eine Erklärung sowie eine inkompatible Änderung, die bestehendes Feld, Norm oder Verbraucherverhalten bricht. Überschreiben Sie eine ältere Version nicht still mit einer inkompatiblen Änderung. Veröffentlichen Sie ein neues Schema mit Änderungsprotokoll, Liste betroffener Datensätze, Alt-zu-Neu-Migrationszuordnung, Kompatibilitätstest, Abkündigungsdatum und Archivbeziehung.

Einfach erklärt

Denken Sie an einen Stadtplan. Einen Schreibfehler im Straßennamen zu korrigieren ist nicht dasselbe wie eine Brücke zu schließen und eine neue Straße zu eröffnen. Wer die neue Route nutzt, braucht Datum, Alternative und den Zeitpunkt, bis zu dem der alte Plan verwendbar bleibt.

Warum ist das wichtig?

Ein Feld still zu löschen oder eine Norm zu verändern kann alte Anwendungen Daten falsch lesen lassen und zwischen Sprachen unterschiedliche Aussagen erzeugen. Eine Versionsnummer genügt nicht; Wirkung und Migrationsweg müssen bekannt sein.

Nicht verwechseln

- Eine Rechtschreibkorrektur ist eine redaktionelle Änderung ohne wesentliche Bedeutungsänderung.
- Eine rückwärtskompatible Ergänzung bietet ein neues Feld oder eine Option, ohne ältere Verbraucher zu brechen.
- Eine inkompatible Schemaänderung kann ältere Verbraucher falsch oder unvollständig arbeiten lassen.
- Eine normative Änderung verändert Gebot oder Verbot; sie ist nicht nur eine technische Schemaänderung.
- Abkündigung ist ein Lebenszyklus mit angekündigtem Ende und Migrationsweg, keine sofortige Feldlöschung.

Was sollten Sie tun?

1. Definieren Sie öffentliche Felder, normative Datensätze und Dateiverträge versioniert.
2. Klassifizieren Sie jede Änderung als redaktionell, rückwärtskompatibel, inkompatibel, normativ oder sicherheitsbezogen.
3. Nennen Sie im Änderungsprotokoll geändertes Feld, Grund, betroffene Datensätze, Datum und Entscheidungsverantwortlichen.
4. Verbinden Sie Menschen-, JSON-, Schema-, API-, PDF- und Sprachversionen mit derselben Freigabeerklärung.
5. Stellen Sie bei inkompatibler Änderung Alt-zu-Neu-Feldzuordnung, Transformationsbeispiel und Migrationswerkzeug oder -anleitung bereit.
6. Kündigen Sie Warnung, Unterstützungszeitraum, Entfernungsdatum und sicheren Rückfallweg an.
7. Testen Sie Rückwärtskompatibilität mit alten Beispielen, Schema und Parität mit neuen Beispielen und archivieren Sie die Freigabe unveränderlich.

Wie wird es geprüft?

- Sind Änderungsklasse und wesentliche Wirkung ausdrücklich benannt?
- Bezeichnet die Versionsnummer auf jeder Oberfläche dieselbe Freigabe?
- Wurde eine inkompatible Änderung als kleine Korrektur verborgen?
- Sind Änderungsprotokoll, betroffene Datensätze und Migrationsweg vollständig?
- Wurde Kompatibilität mit älteren Verbrauchern und Dateien tatsächlich getestet?
- Hat ein abgekündigtes Feld Datum, Warnung und Alternative?
- Ist die alte Version unveränderlich verfügbar und mit der neuen verbunden?

Grenze

> Nummernschemata wie MAJOR.MINOR.PATCH signalisieren Änderungen nützlich, beweisen aber keine Kompatibilität. Dieselbe Änderung kann Buch, Norm, Datensatz und API verschieden betreffen. Sicherheits- oder Rechtsnotwendigkeit kann eine Migrationsfrist verkürzen; Grund und Wirkung sind dennoch zu erfassen.

In einem Satz merken

> Eine neue Freigabe ist nicht nur eine neue Zahl, sondern ein erklärtes Änderungsversprechen.

Quellen: S07, S14, S15, S35, S53, S54, S58

Verwandte Einträge: NGQ-014, NGQ-019, NGQ-021, NGQ-022, NGQ-050, NGQ-064, NGQ-065, NGQ-066, NGQ-068, NGQ-069

NGQ-068 — Wie werden DOI, kanonische URL, Dateihash, Lizenz, Archivspiegel und Versionsbeziehungen in der Verifikationskette eines Werks verwendet?

Kanonische Veröffentlichung, Interoperabilität und Pflege · Eintrag NGQ-068 · Version 0.3.1

> **Kürzeste Antwort** Eine DOI identifiziert das Werk, die kanonische URL weist zur offiziellen Weboberfläche, der Dateihash prüft die Kopie, die Lizenz erklärt zulässige Nutzung, und Beziehungsdatensätze verbinden Versionen.

Direkte Antwort

Ein Kanonisierungspaket führt Identität und Verteilungsfamilie einer Freigabe in einer Erklärung zusammen. Erfassen Sie Werk- oder Versions-DOI, kanonische URL, Titel, Autor, Version, Datum, Dateiname, Größe, Hashalgorithmus und -wert, Lizenz, Archivspiegel und Beziehungstypen. Jede Plattformkopie trägt die richtige Beziehung zum kanonischen Werk. Eine DOI oder die Zahl der Plattformen belegt keine Qualität; ein Dateihash zeigt nur, ob sich die verglichenen Dateibytes unterscheiden.

Einfach erklärt

Stellen Sie sich einen Reisepass für ein Buch vor. Die DOI ist seine dauerhafte Identitätsnummer, die kanonische URL seine offizielle Anschrift, der Dateihash sein Siegelabdruck, die Lizenz seine Nutzungserlaubnis und das Archiv seine bewahrte Kopie. Ein Pass beweist nicht, dass das Buch gut ist; er hilft zu erkennen, welches Werk und welche Kopie vorliegen.

Warum ist das wichtig?

Werden verschiedene Dateien unter demselben Namen veröffentlicht, können Menschen und KI-Systeme die offizielle Version nicht erkennen. Falsche DOI-Beziehung, veraltete Datei oder unklare Lizenz unterbrechen Zitier- und Wiederverwendungskette.

Nicht verwechseln

- Eine Werk-DOI kann eine Werkfamilie mit mehreren Versionen darstellen.
- Eine Versions-DOI identifiziert eine bestimmte unveränderliche Freigabe.
- Die kanonische Webausgabe ist die aktuelle offizielle Menschen- und Maschinenoberfläche des Herausgebers.
- Ein Archivspiegel bewahrt eine Kopie; er muss weder kanonische Veröffentlichung noch unabhängige Verifizierung sein.
- Eine Verteilungskopie unterstützt Auffindbarkeit; ein abgeleiteter Datensatz kann eine eigenständige, aus dem Werk erzeugte Ressource sein.

Was sollten Sie tun?

1. Sperren Sie Menschen- und Maschinendateien für die Freigabe und erfassen Sie Namen, Größen, Medientypen und Hashes.
2. Verknüpfen Sie Werk-DOI, Versions-DOI und kanonische URL wechselseitig mit richtigen Beziehungstypen in den Metadaten.
3. Stimmen Sie Bedeutung von Titel, Autor, Datum, Version, Sprache, Lizenz und Beschreibung plattformübergreifend ab.
4. Klassifizieren Sie jeden Spiegel ausdrücklich als kanonische Veröffentlichung, Version, Archivspiegel, Verteilungskopie oder abgeleiteten Datensatz.
5. Nennen Sie abgedeckte Dateien und Elemente der Lizenz, Ausnahmen für Drittrechte und Zitierform.
6. Berechnen Sie nach dem Download Hashes neu, um Bit-Parität von Archiv- und Verteilungskopien zu prüfen.
7. Führen Sie regelmäßige Verifikationsdatensätze für DOI-Auflösung, kanonische URL, Dateizugang, Metadaten und Hash-Parität.

Wie wird es geprüft?

- Löst die DOI zum richtigen Werk und zur richtigen Version auf?
- Sind Beziehungen zu Werk, Version, Vorgänger, Nachfolger und abgeleiteter Ressource richtig typisiert?
- Ist die kanonische URL ausdrücklich und in Plattformmetadaten einheitlich?
- Stimmen Hashalgorithmus, -wert, Dateiname und Größe?
- Sind Lizenzumfang und Drittrechtsausnahmen verständlich?
- Wurde eine Archiv- oder Verteilungskopie als unabhängige Verifizierung dargestellt?
- Wurden DOI-, Download- oder Plattformzahlen als Beleg akademischer Wirkung oder Annahme verwendet?

Grenze

> Eine DOI belegt für sich allein weder Urheberschaft, Peer Review, Richtigkeit noch weltweite Annahme. Ein Dateihash vergleicht Kopien; er beweist nicht, dass eine Datei richtig, ungefährlich oder rechtmäßig ist. Eine Lizenz kann nur der Rechteinhaber oder eine befugte Partei erteilen; die konkrete Wahl kann Rechtsfolgen haben.

In einem Satz merken

> Identität, Adresse, Integrität, Erlaubnis und Beziehung sind verschieden; gemeinsam bilden sie eine Verifikationskette.

Quellen: S14, S15, S35, S55, S56, S58, S59

Verwandte Einträge: NGQ-014, NGQ-019, NGQ-020, NGQ-021, NGQ-022, NGQ-059, NGQ-064, NGQ-065, NGQ-066, NGQ-067, NGQ-069

NGQ-069 — Wie ist NOMOS-GEO-QA-Konformität zu beschreiben, wer darf den Text ändern, und wie wird das Werk dauerhaft bewahrt?

Kanonische Veröffentlichung, Interoperabilität und Pflege · Eintrag NGQ-069 · Version 0.3.1

> **Kürzeste Antwort** Eine Konformitätserklärung muss Umfang, Version, Belege, Ausnahmen, Prüfer, Datum und Ergebnis zeigen und darf den vorgeschlagenen Status des Frameworks nie verbergen.

Direkte Antwort

Eine Konformitätserklärung bestimmt zuerst den Prüfgegenstand: Datensätze, Version, Sprache, Publikationsoberfläche und Datum. Sie nennt außerdem bestandene Tore, verbleibende Ausnahmen, Prüfungsart, Entscheidungsverantwortlichen und Gültigkeitszeitraum. Selbstbewertung, Kunden- oder Partnerprüfung und unabhängige Drittprüfung sind verschieden und getrennt zu benennen. Ohne echte externe Autorität darf das Werk weder „zertifiziert“ noch „offizieller Standard“ oder „weltweit angenommen“ genannt werden. In der Gründerausgabe liegen abschließende menschliche Genehmigung und Änderungsbefugnis bei Kaan MURAZ. Werden sie später übertragen oder mit einem Gremium geteilt, wird dies durch einen öffentlichen, versionierten Datensatz offengelegt.

Einfach erklärt

Denken Sie an eine Gebäudeprüfbescheinigung. Sie sollte sagen, welche Stockwerke wann von wem geprüft wurden und welche Mängel bestehen bleiben. „Dieses Gebäude ist konform“ genügt nicht. Der Eigentümer darf die eigene Prüfung auch nicht als behördliche Genehmigung darstellen.

Warum ist das wichtig?

Eine mehrdeutige Konformitätsaussage kann einen begrenzten Test wie eine Garantie für das gesamte System erscheinen lassen. Ohne Änderungsbefugnis und Archivplan kann das Werk still verschlechtert, abgespalten oder in einen Standard entgegen der Gründerabsicht verwandelt werden.

Nicht verwechseln

- Selbstbewertung ist die eigene Aussage der Organisation; sie ist keine unabhängige Prüfung.
- Geprüfte Konformität zeigt, dass genannter Umfang und Version nach bestimmter Methode untersucht wurden.
- Unabhängige Annahme bedeutet, dass eine externe Partei das Framework freiwillig nutzt; der Herausgeber kann sie nicht herbeibehaupten.
- Offizieller Standardstatus verlangt ein befugtes Normungsverfahren; Veröffentlichung allein schafft ihn nicht.
- Zertifizierung verlangt eine bestimmte Autorität, ein Schema, Bewertung und Überwachungsprogramm; sie ist nicht dasselbe wie ein gewöhnlicher Prüfbericht.

Was sollten Sie tun?

1. Bestimmen Sie den Konformitätsumfang nach Datensatz, Sprache, Oberfläche, System, Version, Datum und Gültigkeitszeitraum.
2. Nehmen Sie Pflichtore, verwendete Belege, Nichtkompensationsergebnis und Ausnahmen in die Erklärung auf.
3. Klassifizieren Sie die Prüfung richtig als Selbst-, Zweitpartei- oder unabhängige Drittprüfung und legen Sie Interessen offen.
4. Veröffentlichen Sie eine bestimmte Entscheidung wie PASS, CONDITIONAL, FAIL oder UNRESOLVED samt Begründung.
5. Dokumentieren Sie Vorschlag, Prüfung, Gründergenehmigung von Kaan MURAZ, Änderungsprotokoll, Anfechtungs- und Rollback-Wege.
6. Sperren Sie bei jeder Freigabe türkisches Original, sechs Sprachen, Schema, Quellen, Hashes, DOI und Archivbeziehungen.
7. Bewahren Sie bei Delegation, Ende der Pflege oder institutioneller Änderung Steward, Archiv und letzte gültige Freigabe durch einen öffentlichen Datensatz.

Wie wird es geprüft?

- Welche Datensätze, Oberflächen, Sprachen und Versionen deckt die Konformitätserklärung genau ab?
- Sind Belege, Ausnahmen, Gültigkeitsdatum und Entscheidungsverantwortlicher sichtbar?
- Wurde eine Selbstbewertung als unabhängige Prüfung dargestellt?
- Wurde ein kritischer Fehler durch Mittelwert oder Teilerfolg verborgen?
- Gibt es eine falsche externe Autoritätsbehauptung zu offiziellem Standard, Zertifizierung oder weltweiter Annahme?
- Sind Änderungs-, Anfechtungs-, Versions-, Archiv- und Delegationsverfahren praktikabel?
- Lassen sich Gründerabsicht und letzte gültige Freigabe nach Personen- oder Institutionswechsel weiterhin verifizieren?

Grenze

> In dieser Freigabe ist NOMOS GEO-QA ein von NobleJackal vorgeschlagenes Gründerframework; es ist weder ein unabhängig angenommener internationaler offizieller Standard noch ein akkreditiertes Zertifizierungsprogramm. Eine Konformitätserklärung garantiert weder KI-Sichtbarkeit, Zitierung, Ranking oder Rechtskonformität noch schadlose Ergebnisse.

In einem Satz merken

> Der Wert eines Standards liegt nicht darin, wie groß er sich beschreibt, sondern welche Aussage er an welchen Beleg, innerhalb welcher Grenze und unter wessen Verantwortung bindet.

Quellen: S44, S50, S59, S60

Verwandte Einträge: NGQ-001, NGQ-014, NGQ-015, NGQ-026, NGQ-050, NGQ-059, NGQ-061, NGQ-063, NGQ-064, NGQ-065, NGQ-066, NGQ-067, NGQ-068

Kurzglossar

Dieses Glossar erklärt Fachbegriffe, die bei der ersten Lektüre auftreten können. Prüfen Sie bei anbieterspezifischen Begriffen den genauen Geltungsbereich in der jeweils maßgeblichen offiziellen Dokumentation.

KI-System

Ein auf künstlicher Intelligenz beruhendes System, das Eingaben empfängt und Vorhersagen, Klassifizierungen, Inhalte oder Handlungen erzeugt. Gemeint ist kein bestimmtes Produkt oder Modell.

Verwandte Einträge: NGQ-001, NGQ-010, NGQ-032, NGQ-033

Generatives System

Ein System, das als Antwort auf eine Nutzeranfrage Text, Bilder, Audio, Code oder andere Ausgaben erzeugen kann.

Verwandte Einträge: NGQ-001, NGQ-003, NGQ-005

GEO

In diesem Werk die Disziplin, die Bedingungen messbar zu verbessern, unter denen eine Entität in generativen Systemen gefunden, Belegen zugeordnet und korrekt repräsentiert werden kann.

Verwandte Einträge: NGQ-001, NGQ-003, NGQ-012

Entität

Eine Person, Organisation, Marke, ein Produkt, eine Dienstleistung, ein Ort, Werk, Ereignis oder Begriff, der von anderen Personen oder Dingen unterschieden werden muss.

Verwandte Einträge: NGQ-004, NGQ-020, NGQ-023

Digitale Repräsentation

Die Bedeutung, die ein digitales System aus Identität, Merkmalen, Beziehungen, Grenzen, Belegen und Zeitangaben über eine Entität erzeugt.

Verwandte Einträge: NGQ-005, NGQ-006, NGQ-014

Erwähnung

Das Erscheinen des Namens oder eines ausdrücklichen Identitätsmerkmals einer Entität in einer Antwort.

Verwandte Einträge: NGQ-002, NGQ-006, NGQ-012

Zitat

Ein sichtbarer Quellenverweis in einer Antwort. Ob die Quelle die betreffende Aussage tatsächlich stützt, muss getrennt geprüft werden.

Verwandte Einträge: NGQ-006, NGQ-007, NGQ-012

Empfehlung

Darstellung einer Entität als geeignete Möglichkeit für den Nutzer.

Verwandte Einträge: NGQ-006, NGQ-013

Aussage

Ein sachlicher Satz oder Satzteil, der als wahr, falsch, unvollständig oder unsicher bewertet werden kann.

Verwandte Einträge: NGQ-007, NGQ-015

Quelle

Ein Dokument, Datensatz, eine Seite, Datenbank oder andere Publikationsoberfläche, aus der Information stammt.

Verwandte Einträge: NGQ-007, NGQ-008, NGQ-009

Beleg

Ein verifizierbarer Nachweis, der eine bestimmte Aussage innerhalb eines bestimmten Umfangs und Zeitraums tatsächlich stützt.

Verwandte Einträge: NGQ-007, NGQ-008, NGQ-015

Primärquelle

Ein ursprünglicher Datensatz, der unmittelbar mit dem erzeugten Ereignis, der Entscheidung oder Information verbunden ist.

Verwandte Einträge: NGQ-008

Unabhängiger Beleg

Verifizierung durch eine Quelle, die institutionell oder methodisch von der behauptenden Partei getrennt ist.

Verwandte Einträge: NGQ-008, NGQ-009

Informationsabruf

Der Vorgang, bei dem ein System Informationen oder Quellen findet und auswählt, die für eine bestimmte Frage verwendet werden können.

Verwandte Einträge: NGQ-010, NGQ-011, NGQ-017

Crawling

Das Entdecken und Anfordern einer URL durch ein automatisiertes Werkzeug mit dem Versuch, den ausgelieferten Inhalt abzurufen.

Verwandte Einträge: NGQ-016, NGQ-017

Indexierung

Analyse abgerufener Inhalte und ihre Umwandlung in einen Datensatz, der in einem Such- oder Abrufsystem verwendet werden kann.

Verwandte Einträge: NGQ-017

Strukturierte Daten

Markup, das Maschinen die Angaben einer Seite mithilfe bestimmter Felder und Beziehungen erklärt.

Verwandte Einträge: NGQ-018, NGQ-019

JSON

Ein Textformat, das Daten in einer geordneten Struktur aus Schlüsseln und Werten überträgt.

Verwandte Einträge: NGQ-018, NGQ-019

JSON-LD

Eine Möglichkeit, mit JSON die Bedeutung verknüpfter Daten über Entitäten und Beziehungen auszudrücken.

Verwandte Einträge: NGQ-018, NGQ-019, NGQ-020

Kanonische URL

Ein Signal, das unter ähnlichen oder doppelten URLs die bevorzugte Seitenadresse bestimmt.

Verwandte Einträge: NGQ-017, NGQ-019, NGQ-020

Kanonischer Identitätsdatensatz

Der von NOMOS GEO vorgeschlagene Primärdatensatz zur Verwaltung stabiler Identität, Namen, Beziehungen, Status und Belegverknüpfungen einer Entität.

Verwandte Einträge: NGQ-020, NGQ-021, NGQ-022

Kanonischer Name

Der bevorzugte Primärname innerhalb eines bestimmten Datensatzes und Nutzungskontexts.

Verwandte Einträge: NGQ-022

Alternativname

Ein gültiger, vom Primärnamen abweichender Name derselben Entität.

Verwandte Einträge: NGQ-022, NGQ-023

Entitätsauflösung

Der Vorgang, bei dem bestimmt wird, welche reale Entität ein Name oder Datensatz bezeichnet.

Verwandte Einträge: NGQ-004, NGQ-023, NGQ-024

Rolle

Funktion oder Beziehung einer Person oder Identität innerhalb einer Organisation. Eine Rolle verleiht nicht automatisch jede Befugnis.

Verwandte Einträge: NGQ-025, NGQ-028

Befugnis

Erlaubnis oder rechtliche Macht, eine bestimmte Handlung innerhalb festgelegter Grenzen und Bedingungen auszuführen.

Verwandte Einträge: NGQ-025, NGQ-026, NGQ-027

Delegation

Übertragung eines bestimmten Teils der Befugnis einer Partei auf einen anderen Akteur, begrenzt nach Umfang und Dauer.

Verwandte Einträge: NGQ-026, NGQ-032, NGQ-033

Herrenloses Konto

Ein noch bestehendes Konto ohne aktuellen Besitzer oder verantwortliche Person.

Verwandte Einträge: NGQ-030

Schattenberechtigung

Eine Berechtigung, die im formalen Rollendatensatz nicht ausdrücklich sichtbar ist, praktisch aber über einen anderen Weg genutzt werden kann.

Verwandte Einträge: NGQ-030

Restzugang

Zugang, der nach Ende der Aufgabe oder des Bedarfs aktiv bleibt.

Verwandte Einträge: NGQ-028, NGQ-030

Dienstkonto

Ein Konto zum Betrieb einer nichtmenschlichen Arbeitslast.

Verwandte Einträge: NGQ-030, NGQ-031

Service Principal

In Microsoft Entra ein Objekt, das eine Anwendung oder Dienstinstanz als Sicherheitsidentität repräsentiert.

Verwandte Einträge: NGQ-031

Verwaltete Identität

Eine Arbeitslastidentität, deren Zugangsdaten-Lebenszyklus durch einen Cloud-Anbieter verwaltet wird.

Verwandte Einträge: NGQ-031

KI-Agentenidentität

Eine Identität, die einen KI-Agenten mit bestimmtem Zweck, Sponsor, Werkzeugen, Berechtigungen und Handlungsverlauf unterscheidet.

Verwandte Einträge: NGQ-031, NGQ-032, NGQ-033

Technischer Akteur

Die Identität eines Menschen, einer Anwendung, Arbeitslast oder eines Agenten, die eine Handlung in einem System tatsächlich ausführt.

Verwandte Einträge: NGQ-032, NGQ-033

Repräsentiertes Subjekt

Die Person oder Organisation, in deren Namen oder zu deren Nutzen eine Handlung ausgeführt wird.

Verwandte Einträge: NGQ-032

Initiator

Der erste bestimmte Akteur oder das Ereignis, das eine Handlung oder einen Handlungsvorschlag auslöst.

Verwandte Einträge: NGQ-032, NGQ-033

Genehmigender

Die befugte Partei, die eine Handlung für bestimmten Inhalt, Ziel, Umfang und Zeitraum erlaubt.

Verwandte Einträge: NGQ-032, NGQ-033

Ausführender

Der Akteur, der eine genehmigte oder anderweitig befugte Handlung technisch ausführt.

Verwandte Einträge: NGQ-033

Provenienz

Die Beziehungskette, die zeigt, wer einen Datensatz oder eine Handlung aus welchen Eingaben, zu welchem Zeitpunkt und durch welchen Prozess erzeugte.

Verwandte Einträge: NGQ-015, NGQ-029, NGQ-033

Trace-ID

Eine Kennung, die zusammengehörige technische Ereignisse in einer Spur eines verteilten Systems bündelt. Allein belegt sie weder Befugnis noch Richtigkeit.

Verwandte Einträge: NGQ-029, NGQ-033

Menschliche Genehmigung

Erlaubnis einer befugten Person für eine bestimmte Handlung, die versteht, was, warum und mit welcher Folge genehmigt wird.

Verwandte Einträge: NGQ-034, NGQ-035, NGQ-052, NGQ-055

Informierte Genehmigung

Eine Genehmigung, die erst nach verständlicher Darstellung von wesentlichem Zweck, Umfang, Risiken, Alternativen und Folgen erteilt wird.

Verwandte Einträge: NGQ-034, NGQ-036

Handlungsspezifische Genehmigung

Eine auf einen Vorgang mit bestimmtem Ziel, Umfang, Wirkung und Zeitraum begrenzte Genehmigung.

Verwandte Einträge: NGQ-034, NGQ-038, NGQ-055

Wirksame menschliche Aufsicht

Aufsicht, bei der ein Mensch nicht nur auf einer Oberfläche erscheint, sondern Ergebnis prüfen, anfechten, stoppen und ändern kann.

Verwandte Einträge: NGQ-034, NGQ-035, NGQ-036

Automationsbias

Die Neigung, eine automatisierte oder KI-Ausgabe allein wegen ihrer Systemherkunft für richtiger zu halten, als die Belege rechtfertigen.

Verwandte Einträge: NGQ-035, NGQ-036

Abnickentscheidung

Eine formelle Entscheidung, die menschlich genehmigt wirkt, aber keine wirkliche Prüfung, kein Verständnis und keine Änderungsmöglichkeit enthält.

Verwandte Einträge: NGQ-034, NGQ-035

Genehmigungsmüdigkeit

Verlust menschlicher Aufmerksamkeit und Entscheidungsqualität durch zu häufige, unklare oder unnötige Genehmigungsanforderungen.

Verwandte Einträge: NGQ-035

Funktionstrennung

Die Bedingung, dass Befugnis zu Vorbereitung, Genehmigung, Ausführung und Abschluss eines kritischen Vorgangs nicht unangemessen bei einer Partei konzentriert ist.

Verwandte Einträge: NGQ-034, NGQ-038, NGQ-039, NGQ-052, NGQ-063

Entscheidungsspur

Eine Datensatzkette, die Eingabe, Systemversion, Empfehlung, menschliche Prüfung, Genehmigung, Anwendung und Ergebnis einer Entscheidung verbindet.

Verwandte Einträge: NGQ-037, NGQ-041, NGQ-044

Anfechtungsweg

Ein bestimmtes Verfahren, durch das eine betroffene Person eine Entscheidung verstehen und korrigieren sowie eine erneute Prüfung durch eine befugte Person oder unabhängige Stelle erhalten kann.

Verwandte Einträge: NGQ-036, NGQ-037, NGQ-039, NGQ-040

Folgenreiche Entscheidung

Eine Entscheidung, die Rechte, Sicherheit, Lebensunterhalt, wesentliche Leistungen, Ruf oder wichtige Chancen einer Person erheblich beeinflussen kann.

Verwandte Einträge: NGQ-036, NGQ-037, NGQ-038, NGQ-040

Entscheidungslebenszyklus

Alle Stufen einer Entscheidung: Initiierung, Datenerhebung, Erzeugung, Prüfung, Genehmigung, Anwendung, Mitteilung, Anfechtung, Korrektur und Abschluss.

Verwandte Einträge: NGQ-041, NGQ-044

Rückwirkende Neubewertung

Erneute Prüfung früherer Entscheidungen in einem bestimmten Umfang, wenn eine System- oder Bedingungsänderung ein neues Risiko erzeugt.

Verwandte Einträge: NGQ-042, NGQ-043

Historische Richtigkeit

Das Maß, in dem ein Datensatz die bei seiner Erstellung geltenden Informationen und Regeln richtig wiedergibt.

Verwandte Einträge: NGQ-043

Aktuelle Gültigkeit

Ob eine früher richtige Entscheidung oder Information heute weiterhin gültig verwendet werden kann.

Verwandte Einträge: NGQ-042, NGQ-043

Nur ergänzbarer Datensatz

Ein Datensatzmodell, bei dem frühere Ereignisse nicht still überschrieben und neue Zustände als getrennte, geordnete Ereignisse hinzugefügt werden.

Verwandte Einträge: NGQ-044, NGQ-045

Verteilungsbestätigung

Ein Beleg, der zeigt, wann eine Korrektur oder Beschränkung ein Folgesystem erreichte und wie sie dort angewendet wurde.

Verwandte Einträge: NGQ-045, NGQ-046, NGQ-049

Wiederauferstehungsrisiko

Das Risiko, dass gelöschte, berichtigte oder eingeschränkte Daten aus Cache, Sicherung, Export oder Modellgedächtnis erneut erscheinen.

Verwandte Einträge: NGQ-046, NGQ-047, NGQ-048

Löschung

Entfernung von Daten aus einer bestimmten aktiven oder Speicheroberfläche, sodass sie nicht wiederhergestellt oder verwendet werden können; der genaue Umfang richtet sich nach technischem und rechtlichem Kontext.

Verwandte Einträge: NGQ-046, NGQ-047, NGQ-048

Legal Hold

Eine eng begrenzte, dokumentierte Aufbewahrungspflicht, die gewöhnliche Löschung aus einem konkreten rechtlichen oder beweissichernden Grund aussetzt.

Verwandte Einträge: NGQ-047

Medienbereinigung

Der Vorgang, Information auf einem Datenträger unter bestimmten Bedrohungs- und Wiederverwendungsbedingungen unzugänglich zu machen.

Verwandte Einträge: NGQ-048

Maschinelles Verlernen

Ein technischer Vorgang zur Verringerung oder Entfernung des Einflusses bestimmter Trainingsdaten auf das Modellverhalten; er ist nicht dasselbe wie die Löschung eines Datensatzes.

Verwandte Einträge: NGQ-048, NGQ-049, NGQ-050

Nichtverwendungsregel

Eine vorübergehende Kontrolle, die bestimmte Daten von Abruf, Entscheidungen, Training, Empfehlungen oder Werkzeugnutzung fernhält, solange Löschung oder Verlernen unvollständig ist.

Verwandte Einträge: NGQ-049, NGQ-050

Freigabetor

Eine Kontrolle, die bestimmte Tests und menschliche Genehmigung verlangt, bevor Daten, Modell oder Funktion erneut genutzt werden dürfen.

Verwandte Einträge: NGQ-050, NGQ-052

Offener Status

Ein vorübergehender Zustand ohne abschließende Entscheidung, in dem Verantwortlicher, Grund, nächster Schritt, Frist und Eskalationsweg erfasst sein müssen.

Verwandte Einträge: NGQ-051

Sicheres Abschalten

Ein aufgezeichneter Abschaltvorgang, der ein bestimmtes Risiko unterbricht, den betroffenen Umfang begrenzt, Belege bewahrt und sichere Leistungsalternativen berücksichtigt.

Verwandte Einträge: NGQ-052, NGQ-058

Neustarttor

Eine Kontrolle, die eine Wiedereröffnung des Systems verhindert, bis Ursache, Abhilfe, Tests, menschliche Genehmigung und Rollback-Bereitschaft vollständig sind.

Verwandte Einträge: NGQ-052

Prompt Injection

Der Versuch einer Eingabe, ein KI-System aus seinen vorgesehenen Anweisungen, Richtlinien oder Befugnisgrenzen zu drängen.

Verwandte Einträge: NGQ-053

Indirekte Prompt Injection

Übermittlung einer böswilligen Anweisung durch externe Inhalte wie Webseite, Dokument, E-Mail, Bild, Werkzeugausgabe oder Abrufquelle.

Verwandte Einträge: NGQ-053

Quellenvergiftung

Verunreinigung von Quellen in einer Abruf- oder Entscheidungsumgebung, die das System fehlleitet.

Verwandte Einträge: NGQ-054, NGQ-058

Synthetischer Konsens

Der Anschein vieler unabhängiger Quellen und einer gemeinsamen Auffassung, der durch Kopien derselben Ursprungsquelle entsteht.

Verwandte Einträge: NGQ-054

Quellenwäsche

Der Vorgang, eine schwache oder unbelegte Aussage durch Kopier- und Zitierketten glaubwürdig erscheinen zu lassen.

Verwandte Einträge: NGQ-054

KI-Lieferkette

Die Kette externer Bestandteile aus Modellen, Datensätzen, APIs, Plug-ins, Werkzeugen, Infrastruktur und ihren Unterabhängigkeiten.

Verwandte Einträge: NGQ-057

KI- oder Repräsentationsvorfall

Ein Ereignis in einem KI-System oder einer verbundenen Publikations-, Daten- und Werkzeugkette, das durch Falschrepräsentation, Sicherheit, Datenschutz, Befugnis, Leistung oder Belegintegrität Schaden verursacht.

Verwandte Einträge: NGQ-052, NGQ-058

Truth Pack

Ein versioniertes Belegpaket, das atomare Aussagen, Quellen, Konflikte, Umfang, Zeit und als Prüfreferenz verwendete menschliche Urteile verbindet.

Verwandte Einträge: NGQ-059, NGQ-061, NGQ-063

Referenzwahrheit

Die nach einer geeigneten Belegmethode für bestimmte Entität, Umfang, Zeit und Nutzungskontext angenommene Prüfreferenz.

Verwandte Einträge: NGQ-059

Fragenregister

Ein vor dem Test versionierter Bestand aus Fragetexten, Absichten, Risikoklassen und Ausführungsbedingungen.

Verwandte Einträge: NGQ-060, NGQ-064

Atomare Aussage

Der kleinste wesentliche Satz, der für sich verifiziert oder als ungeklärt belassen werden kann.

Verwandte Einträge: NGQ-059, NGQ-061, NGQ-064

Aussageledger

Ein versionierter Datensatz, der für jede atomare Aussage Verknüpfungen zu Entität, Beleg, Ergebnis, Schwere, Prüfer, Begründung und Unsicherheit bewahrt.

Verwandte Einträge: NGQ-061

Nichtkompensation

Der Grundsatz, dass ein kritisches Scheitern nicht durch viele Erfolge mit geringer Wirkung weggemittelt werden kann.

Verwandte Einträge: NGQ-061, NGQ-064, NGQ-069

Ausgabestreuung

Abweichungen von KI-Ausgaben über Zeit und Wiederholungen unter gleichen oder ähnlichen Bedingungen.

Verwandte Einträge: NGQ-060, NGQ-062

Messunsicherheit

Unsicherheit eines Ergebnisses aufgrund von Stichprobe, Bedingungsunterschieden, Klassifizierung und methodischen Grenzen.

Verwandte Einträge: NGQ-062

Konfidenzintervall

Ein statistisches Intervall, das die Messunsicherheit einer Schätzung unter angegebenen Annahmen zusammenfasst; es ist keine Konfidenzaussage des Modells selbst.

Verwandte Einträge: NGQ-062

Prüfungsunabhängigkeit

Eine Arbeitsbedingung, die das Urteil des Prüfers vor unzulässigem Druck schützt, Interessen offenlegt und verhindert, dass er die eigene Arbeit allein genehmigt.

Verwandte Einträge: NGQ-063, NGQ-069

Reproduzierbarkeit

Die Fähigkeit eines anderen hinreichend kompetenten Prüfers, ausgewählte Ergebnisse mit demselben Protokoll und denselben Belegen in angemessenem Maß nachzuvollziehen.

Verwandte Einträge: NGQ-041, NGQ-060, NGQ-063

Abhilfebestätigung

Ein Datensatz, der Fehler, Ursache, Änderung, Bereitstellung, Live-Verifikation, Nachtest, Regression und Abschlussbeleg unter einer Kennung verbindet.

Verwandte Einträge: NGQ-058, NGQ-064

Regression

Ein neuer Fehler, den eine Korrektur in angrenzendem Datensatz, Sprache, Oberfläche, Funktion oder Nutzerweg einführt.

Verwandte Einträge: NGQ-064, NGQ-067

Feldparität

Die wesentliche Gleichwertigkeit bindender Felder wie Identität, Aussage, normative Kraft, Version, Datum, Quellen, Lizenz und Grenzen über Publikationsoberflächen hinweg.

Verwandte Einträge: NGQ-065, NGQ-066

Kontrollierte Transkreation

Sprachübertragung, die natürlichen Zielsprachentext erzeugt und zugleich atomare Aussagen, normative Kraft, Belegumfang, rechtliche Grenzen und Maschinenfeldparität bewahrt.

Verwandte Einträge: NGQ-066

Rückwärtskompatibilität

Die Fähigkeit einer neuen Freigabe, definiertes Verhalten älterer Verbraucher und Dateien nicht zu brechen.

Verwandte Einträge: NGQ-067

Inkompatible Änderung

Eine Änderung, die ein bestehendes Feld, eine Norm, einen Vertrag oder Verbraucherverhalten inkompatibel macht.

Verwandte Einträge: NGQ-067

Migrationszuordnung

Eine versionierte Zuordnung, die die Umwandlung zwischen alten und neuen Feldern, Werten, Regeln und Dateistrukturen erklärt.

Verwandte Einträge: NGQ-067

Abkündigung

Kontrollierte Stilllegung eines Feldes oder einer Freigabe mit Warnung, Alternative, Unterstützungszeitraum und Entfernungsdatum.

Verwandte Einträge: NGQ-067

Kanonisierungspaket

Ein Paket, das Identität, kanonische Adresse, DOI-Beziehungen, Dateien, Hashes, Lizenz und Archivspiegel einer Freigabe in einem Manifest verbindet.

Verwandte Einträge: NGQ-068

Dateiintegritätshash

Ein mit bestimmtem Algorithmus berechneter Prüfwert zur Feststellung, ob sich die verglichene Bytefolge geändert hat.

Verwandte Einträge: NGQ-064, NGQ-068

Konformitätserklärung

Ein Ergebnisdatensatz, der geprüfte Datensätze, Sprachen, Oberflächen, Systeme, Versionen, Daten, Tore, Ausnahmen, Prüfungsart und Entscheidungsverantwortlichen ausdrücklich nennt.

Verwandte Einträge: NGQ-063, NGQ-069

Stewardship und Pflege

Die Regelung, die Gründerabsicht, Zugänglichkeit, Versionsgeschichte und letzten gültigen Zustand des Werks bei Personen- oder Institutionswechseln bewahrt.

Verwandte Einträge: NGQ-068, NGQ-069

Katalog der Primärquellen

Dieser Katalog nennt die wichtigsten Quellen für externe technische, rechtliche und methodische Aussagen. Die Aufnahme einer Quelle bedeutet nicht, dass die jeweilige Institution jede NOMOS-GEO-Definition oder -Regel unterstützt. Prüfen Sie Onlinequellen von Anbietern und Rechtsquellen zum Zeitpunkt der Verwendung erneut.

S01 — Aggarwal et al., GEO: Generative Engine Optimization

Klasse: Forschung · Wichtigste Einträge: NGQ-001, 003, 012, 013

https://arxiv.org/abs/2311.09735

S02 — Google Search Central, SEO Starter Guide

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-001, 003, 010, 013

https://developers.google.com/search/docs/fundamentals/seo-starter-guide

S03 — Google Search Central, Overview of Crawling and Indexing

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-010, 011, 016, 017

https://developers.google.com/search/docs/crawling-indexing

S04 — Google Search Central, Block Search Indexing with noindex

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-016, 017

https://developers.google.com/search/docs/crawling-indexing/block-indexing

S05 — Google Search Central, Introduction to Structured Data

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-018, 019

https://developers.google.com/search/docs/appearance/structured-data/intro-structured-data

S06 — Google Search Central, General Structured Data Guidelines

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-018, 019

https://developers.google.com/search/docs/appearance/structured-data/sd-policies

S07 — W3C, JSON-LD 1.1

Klasse: Standard · Wichtigste Einträge: NGQ-018, 019, 020

https://www.w3.org/TR/json-ld11/

S08 — Schema.org, Data Model

Klasse: Standard- und Community-Vokabular · Wichtigste Einträge: NGQ-004, 018–024

https://schema.org/docs/datamodel.html

S09 — OpenAI, Overview of OpenAI Crawlers

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-016

https://developers.openai.com/api/docs/bots

S10 — Anthropic, Does Anthropic Crawl Data from the Web?

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-016

https://support.anthropic.com/en/articles/8896518-does-anthropic-crawl-data-from-the-web-and-how-can-site-owners-block-the-crawler

S11 — Google Search Central, Canonicalization

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-019–021

https://developers.google.com/search/docs/crawling-indexing/consolidate-duplicate-urls

S12 — ORCID, ORCID Trust

Klasse: Identitätsinfrastruktur · Wichtigste Einträge: NGQ-020–023

https://info.orcid.org/orcid-trust/

S13 — ROR, ROR Data Structure

Klasse: Identitätsinfrastruktur · Wichtigste Einträge: NGQ-020–023

https://ror.readme.io/docs/ror-data-structure

S14 — DataCite, Versioning

Klasse: Identitätsinfrastruktur · Wichtigste Einträge: NGQ-020–022

https://support.datacite.org/docs/versioning

S15 — DataCite, Connecting Versions with Related Identifiers

Klasse: Identitätsinfrastruktur · Wichtigste Einträge: NGQ-020–022

https://support.datacite.org/docs/connecting-versions-with-related-identifiers

S16 — IETF, RFC 5646, Tags for Identifying Languages

Klasse: Standard · Wichtigste Einträge: NGQ-022

https://www.rfc-editor.org/info/rfc5646/

S17 — Wikidata, Help: Statements

Klasse: Identitätsinfrastruktur · Wichtigste Einträge: NGQ-023

https://www.wikidata.org/wiki/Help:Statements/en

S18 — WIPO, Trademarks

Klasse: Offizielle Behörde · Wichtigste Einträge: NGQ-024

https://www.wipo.int/en/web/trademarks

S19 — Handelsministerium der Republik Türkei, Unternehmens- und Handelsregisterrecht

Klasse: Offizielle Behörde · Wichtigste Einträge: NGQ-025–029

https://www.ticaret.gov.tr/ic-ticaret/mevzuat/sirketler-ve-ticaret-sicili

S20 — Handelsministerium der Republik Türkei, Handelsregister

Klasse: Offizielle Behörde · Wichtigste Einträge: NGQ-025–029

https://ticaret.gov.tr/ic-ticaret/ticaret-sicili

S21 — Türkisches Handelsgesetzbuch Nr. 6102, vom Ministerium bereitgestellte PDF-Fassung

Klasse: Offizielle Behörde · Wichtigste Einträge: NGQ-025–028

https://ticaret.gov.tr/data/5d419b8013b87639ac9e00cd/17d7c7108dae78d14a3f220b519f98f6.pdf

S22 — Handelsministerium der Republik Türkei, MERSİS — Zentrales Registersystem

Klasse: Offizielle Behörde · Wichtigste Einträge: NGQ-025–030

https://ticaret.gov.tr/ic-ticaret/ticaret-sicili/merkezi-sicil-kayit-sistemi-mersis

S23 — Behörde für Informations- und Kommunikationstechnologien (BTK), Elektronische Signatur — Allgemeine Informationen

Klasse: Offizielle Behörde · Wichtigste Einträge: NGQ-026, 027, 032, 033

https://btk.gov.tr/elektronik-imza-genel-bilgi

S24 — NIST SP 800-63-4, Digital Identity Guidelines

Klasse: Standard · Wichtigste Einträge: NGQ-028–033

https://csrc.nist.gov/pubs/sp/800/63/4/final

S25 — NIST SP 800-63B-4, Authentication and Authenticator Management

Klasse: Standard · Wichtigste Einträge: NGQ-028–031

https://pages.nist.gov/800-63-4/sp800-63b.html

S26 — NIST SP 800-53 Rev. 5, Security and Privacy Controls

Klasse: Standard · Wichtigste Einträge: NGQ-028–033

https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

S27 — IETF, RFC 7644, System for Cross-domain Identity Management: Protocol

Klasse: Standard · Wichtigste Einträge: NGQ-028–030

https://www.rfc-editor.org/info/rfc7644/

S28 — IETF, RFC 9967, SCIM Roles and Entitlements Extension

Klasse: Standard · Wichtigste Einträge: NGQ-028–030

https://www.rfc-editor.org/info/rfc9967/

S29 — Microsoft Learn, Application and Service Principal Objects in Microsoft Entra ID

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-030–032

https://learn.microsoft.com/en-us/entra/identity-platform/app-objects-and-service-principals

S30 — Microsoft Learn, Managed Identities for Azure Resources

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-030–032

https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview

S31 — Google Cloud, Identities for Workloads

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-030–032

https://docs.cloud.google.com/iam/docs/workload-identities

S32 — AWS IAM, Temporary Credentials with AWS Resources

Klasse: Anbieterdokumentation · Wichtigste Einträge: NGQ-030–032

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_use-resources.html

S33 — IETF, RFC 6749, The OAuth 2.0 Authorization Framework

Klasse: Standard · Wichtigste Einträge: NGQ-031, 032

https://www.rfc-editor.org/info/rfc6749/

S34 — IETF, RFC 8693, OAuth 2.0 Token Exchange

Klasse: Standard · Wichtigste Einträge: NGQ-032, 033

https://www.rfc-editor.org/info/rfc8693/

S35 — W3C, PROV-O: The PROV Ontology

Klasse: Standard · Wichtigste Einträge: NGQ-021, 029, 032, 033

https://www.w3.org/TR/prov-o/

S36 — W3C, Trace Context

Klasse: Standard · Wichtigste Einträge: NGQ-029, 033

https://www.w3.org/TR/trace-context/

S37 — OpenTelemetry, General Trace Semantic Conventions

Klasse: Standard- und Projektdokumentation · Wichtigste Einträge: NGQ-029, 033

https://opentelemetry.io/docs/specs/semconv/general/trace/

S38 — NIST AI 600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile

Klasse: Freiwilliger, standardorientierter institutioneller Leitfaden · Wichtigste Einträge: NGQ-052, 056–058

https://doi.org/10.6028/NIST.AI.600-1

S39 — NIST AI 100-2 E2025, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations

Klasse: Freiwilliger, standardorientierter institutioneller Leitfaden · Wichtigste Einträge: NGQ-053–055

https://doi.org/10.6028/NIST.AI.100-2e2025

S40 — OWASP GenAI Security Project, LLM01:2025 Prompt Injection

Klasse: Offener Leitfaden eines Sicherheitsprojekts · Wichtigste Einträge: NGQ-053

https://genai.owasp.org/llmrisk/llm01-prompt-injection/

S41 — NCSC und Partnerbehörden, Guidelines for Secure AI System Development

Klasse: Offizieller behördenübergreifender Sicherheitsleitfaden · Wichtigste Einträge: NGQ-052–058

https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development/guidelines

S42 — NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management

Klasse: Freiwilliger, standardorientierter institutioneller Leitfaden · Wichtigste Einträge: NGQ-052, 058

https://doi.org/10.6028/NIST.SP.800-61r3

S43 — NIST SP 800-161 Rev. 1 Update 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Klasse: Freiwilliger, standardorientierter institutioneller Leitfaden · Wichtigste Einträge: NGQ-054, 057

https://doi.org/10.6028/NIST.SP.800-161r1-upd1

S44 — NIST, AI Risk Management Framework Playbook und AI RMF Core

Klasse: Freiwilliger Umsetzungsleitfaden · Wichtigste Einträge: NGQ-052–058

https://airc.nist.gov/airmf-resources/playbook/

S45 — Europäische Union, Verordnung (EU) 2024/1689 — Gesetz über künstliche Intelligenz

Klasse: Rechtsvorschrift · Wichtigste Einträge: NGQ-052, 055, 057, 058

https://eur-lex.europa.eu/eli/reg/2024/1689/oj

S46 — European Data Protection Board, Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models

Klasse: Offizielle Stellungnahme eines Gremiums · Wichtigste Einträge: NGQ-056

https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

S47 — NIST, Privacy Framework 1.0: A Tool for Improving Privacy through Enterprise Risk Management

Klasse: Freiwilliges Rahmenwerk für Datenschutzrisiken · Wichtigste Einträge: NGQ-056, 057

https://doi.org/10.6028/NIST.CSWP.01162020

S48 — Europäische Union, Verordnung (EU) 2016/679 — Datenschutz-Grundverordnung

Klasse: Rechtsvorschrift · Wichtigste Einträge: NGQ-056, 058

https://eur-lex.europa.eu/eli/reg/2016/679/oj

S49 — Türkische Datenschutzbehörde, Gesetz Nr. 6698 zum Schutz personenbezogener Daten

Klasse: Offizielle Behörde und Rechtsvorschrift · Wichtigste Einträge: NGQ-056, 058

https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

S50 — NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0)

Klasse: Freiwilliges, standardorientiertes institutionelles Rahmenwerk · Wichtigste Einträge: NGQ-059–NGQ-064

https://doi.org/10.6028/NIST.AI.100-1

S51 — NIST/SEMATECH, e-Handbook of Statistical Methods

Klasse: Technisches Handbuch einer offiziellen Behörde · Wichtigste Einträge: NGQ-060, NGQ-062

https://www.itl.nist.gov/div898/handbook/

S52 — NIST CSWP 31, Proxy Validation and Verification for Critical AI Systems: A Proxy Design Process

Klasse: Technisches Weißbuch einer offiziellen Behörde · Wichtigste Einträge: NGQ-060, NGQ-063, NGQ-064

https://doi.org/10.6028/NIST.CSWP.31

S53 — JSON Schema, Specification — Draft 2020-12

Klasse: Offene technische Spezifikation · Wichtigste Einträge: NGQ-065, NGQ-067

https://json-schema.org/specification

S54 — Semantic Versioning 2.0.0

Klasse: Offene Spezifikation zur Versionierung · Wichtigste Einträge: NGQ-067

https://semver.org/spec/v2.0.0.html

S55 — DOI Foundation, DOI Handbook

Klasse: Offizielles Handbuch für dauerhafte Identifikatoren · Wichtigste Einträge: NGQ-068

https://www.doi.org/doi-handbook/html/

S56 — NIST FIPS 180-4, Secure Hash Standard

Klasse: Offizieller Standard · Wichtigste Einträge: NGQ-068

https://doi.org/10.6028/NIST.FIPS.180-4

S57 — W3C Internationalization, Declaring Language in HTML

Klasse: W3C-Umsetzungsleitfaden · Wichtigste Einträge: NGQ-066

https://www.w3.org/International/questions/qa-html-language-declarations

S58 — Zenodo, About Records

Klasse: Offizielle Repository-Dokumentation · Wichtigste Einträge: NGQ-067, NGQ-068

https://help.zenodo.org/docs/deposit/about-records/

S59 — Creative Commons, About CC Licenses und License Chooser

Klasse: Offizielle Dokumentation des Lizenzanbieters · Wichtigste Einträge: NGQ-068, NGQ-069

https://creativecommons.org/share-your-work/cclicenses/

S60 — IETF BCP 14 / RFC 8174, Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words

Klasse: Standard · Wichtigste Einträge: NGQ-066, NGQ-069

https://www.rfc-editor.org/info/rfc8174

S61 — Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225)

Klasse: Internationales Übereinkommen und offizielle Institution · Wichtigste Einträge: NGQ-037–039, NGQ-051

https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

S62 — European Data Protection Board, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679

Klasse: Offizieller Leitfaden eines Gremiums · Wichtigste Einträge: NGQ-034–039, NGQ-047–051

https://www.edpb.europa.eu/documents/guideline/automated-decision-making-and-profiling_en

S63 — NIST SP 800-88 Rev. 2, Guidelines for Media Sanitization

Klasse: Offizieller, standardorientierter Behördenleitfaden · Wichtigste Einträge: NGQ-047, NGQ-048

https://doi.org/10.6028/NIST.SP.800-88r2

S64 — Türkische Datenschutzbehörde, Verordnung über die Löschung, Vernichtung oder Anonymisierung personenbezogener Daten

Klasse: Offizielle Behörde und Rechtsvorschrift · Wichtigste Einträge: NGQ-047–050

https://www.kvkk.gov.tr/Icerik/5441/KISISEL-VERILERIN-SILINMESI-YOK-EDILMESI-VEYA-ANONIM-HALE-GETIRILMESI-HAKKINDA-YONETMELIK

Schlusshinweis und redaktionelle Verantwortung

Diese Ausgabe führt 69 kanonische Einträge in einer kontrollierten deutschen Transkreation zusammen. Die menschliche Lesefassung, die Auditfragen, der Quellenkatalog und die maschinenlesbare Datensatzfamilie werden unter denselben Kennungen geführt.

> **Schlussprinzip** Der Wert eines Frameworks liegt nicht darin, wie groß es von sich spricht, sondern darin, welche Aussage es an welchen Beleg, innerhalb welcher Grenze und unter wessen Verantwortung bindet.